AVIATION SECURITY CHALLENGES: IS TSA READY FOR THE THREATS OF TODAY?

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

JULY 29, 2015

Serial No. 114–30

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE

97–919 PDF WASHINGTON : 2016

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

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

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

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

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

CONTENTS

Page

STATEMENTS

The Honorable Michael T. McCaul, a Representative in Congress From the State of Texas, and Chairman, Committee on Homeland Security:
Oral Statement 1
Prepared Statement 3
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:
Oral Statement 4
Prepared Statement 5
The Honorable Sheila Jackson Lee, a Representative in Congress From the State of Texas:
Prepared Statement 6

WITNESS

Mr. Peter V. Neffenger, Administrator, Transportation Security Administration, U.S. Department Homeland Security:
Oral Statement 8
Prepared Statement 10

FOR THE RECORD

The Honorable Sheila Jackson Lee, a Representative in Congress From the State of Texas:
Article 21

APPENDIX

Questions From Hon. Scott Perry for Peter V. Neffenger 35
Questions From Ranking Member Bennie G. Thompson for Peter V. Neffenger 37

AVIATION SECURITY CHALLENGES: IS TSA READY FOR THE THREATS OF TODAY?

Wednesday, July 29, 2015

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The committee met, pursuant to call, at 10:10 a.m., in Room 311, Cannon House Office Building, Hon. Michael T. McCaul [Chairman of the committee] presiding.

Present: Representatives McCaul, Rogers, Perry, Katko, Carter, Walker, Ratcliffe, Donovan, Thompson, Jackson Lee, Keating, Vela, Watson Coleman, Rice, and Torres.

Chairman MCCAUL. The Committee on Homeland Security will come to order.

Committee is meeting today to provide Members with an opportunity to hear from the newly-confirmed Transportation Security Administrator Peter Neffenger on his plans for leading the TSA. We expect to explore a range of issues related to the operations of the TSA.

I now recognize myself for an opening statement.

Two weeks ago, a terrorist attack in America's heartland, inspired by a hateful ideology, killed 5 American soldiers on U.S. soil, just a day after we marked up the Countering Violent Extremism bill out of this committee.

Fourteen years after 9/11 not only are we still under threat from Islamist terrorists, but they have gone on the defensive globally and expanded their footprint. Radicalization is on the rise and the war is being brought to our doorsteps at a terrifying speed.

We have long known that our aviation sector is a crown jewel of terrorist targets. So as we stare down these real and growing threats, Congress and the American people need confidence in our defenses. In the past few months, TSA has given us concern rather than confidence. Terrorists have to be right only once, and we have to be right 100 percent of the time.

As millions of travelers from all over the world pass through our Nation's airports, the American people must know and trust that the procedures and policies put in place make it safer.

In June, we learned through leaked reports from the Department of Homeland Security's Office of Inspector General that TSA's passenger screening was wrong 96 percent of the time, and that 73 aviation workers have potential ties to terrorism. These findings shatter public confidence. A reported 96 percent failure rate to detect explosives is completely unacceptable.

Administrator Neffenger has an opportunity, I believe, to turn this ship around. As an admiral, I think he has that capability as well. In our discussions that we have had over the past few days, he has displayed candor and an open mind in his approach to this critical position.

In my opinion, TSA needs to do three things in order to move forward to a new chapter. No. 1, restore public confidence. No. 2, enhance risk-based security. No. 3, better leverage the private sector.

We have seen a large expansion of risk-based security initiatives since 2011, however, we still need to do more. TSA's PreCheck program has been in place for 4 years, however, currently only 4 percent of travelers are members of this program. TSA needs to increase its population so that it can focus its efforts on more thoroughly screening those passengers who are unknown and pose a higher risk.

I would like to explore how TSA can better leverage the private sector. The private sector plays a critical role in securing our Nation's aviation system. TSA does not and cannot fulfill its mission alone. The private sector is a necessary partner that TSA needs to continue to rely on in order to successfully fulfill its mission.

TSA and the Department need to look to the future and give the private sector a road map and a vision of what screening will look like 5, 10, and even 15 years from now. The admiral and I have had some very good discussions on that point.

This can help companies developing technologies meet these needs. We cannot expect private companies to invest tens of millions of dollars if we cannot provide them with any certainty or vision on a return on their investment.

Additionally, TSA needs to make necessary reforms in order to enhance the Screening Partnership Program. These partnerships allow airports to hire private screeners instead of Government employees. This program has been in place since 2004 and, yet, TSA is still unable to do an accurate cost comparison that takes into account the full cost of a Federal employee compared to a private-sector employee doing the same job. This gap allows TSA to argue that private screeners do not save the taxpayer money although this is not a fair and accurate accounting assessment.

This committee is dedicated to reforming TSA. We proved our commitment to this effort by passing four important pieces of legislation on the House floor just this Monday that will keep Americans safe.

This legislation came out of this committee as a result of the recent TSA failures. Specifically, these bills will help strengthen and secure the PreCheck program, improve the vetting process for aviation employees, help keep our airport screening equipment better maintained, and implement better accountability policies at local airports for contractors.

But the bottom line is this: The threat is evolving. But Americans are concerned that TSA is not keeping up with that threat.

Administrator Neffenger, you have a tough job ahead of you to lead this agency but we have confidence in you, and we look forward to working with you in these joint efforts to reform TSA, and together today we are eager to hear from you about your plans for the future and your vision.

[The statement of Chairman McCaul follows:]

STATEMENT OF CHAIRMAN MICHAEL T. MCCAUL

JULY 29, 2015

Two weeks ago, a terrorist struck in America's heartland—inspired by a hateful ideology—and killed 5 American soldiers on U.S. soil. Fourteen years after 9/11, not only are we still under threat from Islamist terrorists, but they have gone on the offensive globally and expanded their footprint. Radicalism is on the rise, and the war is being brought to our doorsteps at terrifying speed.

We have long known that our aviation sector is the crown jewel of terrorist targets, so as we stare down these real and growing threats, Congress and the American people need confidence in our defenses. In the past few months, TSA has given us concern rather than confidence. Terrorists have to be right only once, and we have to be right 100% of the time. As millions of travelers from all over the world pass through our Nation's airports, the American people must know and trust that the procedures and policies put in place make us safer.

In June, we learned through leaked reports from the Department of Homeland Security's Office of Inspector General, that TSA's passenger screening was wrong 96% of the time, and that 73 aviation workers had potential ties to terrorism. These findings shatter public confidence. A reported 96% failure rate to detect explosives is completely unacceptable.

Administrator Neffenger has an opportunity to right this ship. In our discussions, he has displayed candor, and an open mind in his approach to this critical position. In my opinion, TSA needs to do three things in order to move forward to a new chapter: (1) Restore public confidence, (2) enhance risk-based security; and (3) better leverage the private sector.

We have seen a large expansion of risk-based security initiatives since 2011; however, we still need to do more. TSA's PreCheck program has been in place for 4 years, however, currently only 4% of travelers are members of this program. TSA needs to increase this population, so that it can focus its efforts on more thoroughly screening those passengers who are unknown and pose a bigger risk.

I would like to explore how TSA can better leverage the private sector. The private sector plays a critically important role in securing our Nation's aviation system. TSA does not and cannot fulfill its mission alone. The private sector is a necessary partner that TSA needs to continue to rely on in order to successfully fulfill its mission.

TSA and the Department need to look to the future and give the private sector a roadmap of what screening will look like 5, 10, and 15 years from now. This can help companies developing technologies meet these needs. We cannot expect private companies to invest tens of millions of dollars, if we cannot provide them any certainty on a return on their investment.

Additionally, TSA needs to make necessary reforms in order to enhance the Screening Partnership Program. These partnerships allow airports to hire private screeners instead of Government employees. This program has been in place since 2004, and yet TSA is still unable to do an accurate cost comparison that takes into account the full cost of a Federal employee compared to a private-sector employee doing the same job.

This gap allows TSA to argue that private screeners do not save the taxpayer money, although this is not a fair and accurate accounting assessment. This committee is dedicated to reforming TSA. We proved our commitment to this effort by passing four important pieces of legislation on the House floor on Monday that will keep Americans safe.

This legislation came out of this committee as a result of the recent TSA failures. Specifically, these bills will help strengthen and secure the PreCheck program, improve the vetting process for aviation employees, help keep our airport screening equipment better maintained and implement better accountability policies at local airports for contractors.

The bottom line is this: The threat is evolving, but Americans are concerned that TSA is not keeping up. Administrator Neffenger, you have a tough job ahead of you to lead this agency. But we look forward to working with you to reform TSA—and today we are eager to hear about your plans to do exactly that.

Chairman MCCAUL. With that, the Chair now recognizes the Ranking Member.

Mr. THOMPSON. Thank you very much, Mr. Chairman, for holding this hearing. I would also like to congratulate Administrator Neffenger on his appointment, and I look forward to working with him to advance the mission of TSA.

Another thing is, you say, "Welcome to the fish bowl."

[Laughter.]

TSA was established by Congress in the wake of the September 11 attack. It has responsibility for protecting the Nation's surface and aviation transportation systems and ensuring the free movement of people and goods.

Over the years in protecting aviation systems, TSA has used a number of methods to screen passengers. Some of the technological changes TSA has made, however, have cost taxpayers millions of dollars while failing to adequately address the threat to aviation security.

Unfortunately, TSA is still having problems with its technology today. For example, last month, it was reported that auditors posing as passengers were able to smuggle mock explosives and banned weapons through checkpoints at various airports across the country.

Earlier this spring, the inspector general released a report claiming that TSA does not properly manage the maintenance of its airport screening equipment. According to the I.G., TSA has not issued adequate policies to airports for carrying out maintenance responsibility.

Administrator Neffenger, I want to challenge you to address these issues with the technologies used in the airport environment. As you approach this issue, consider both the current threat picture and the emerging threats. Keep in mind that there are small and minority businesses in this country with exceptional technologies that could be beneficial to TSA and improve efficiencies at the airport.

I highlight that because we have gotten accustomed to using three or four vendors and every time we have come before this committee, somebody would say, well, they are the only someone with capacity to do what we need. My question is: Well, how hard have we looked and how cooperative have we been with other people who are in this arena? So I look forward to working with you on that.

Former Administrator Pistole implemented a risk-based approach to passenger screening. However, both the Government Accountability Office and the Office of Inspector General have identified shortcomings with this approach, especially when it comes to granting passengers expedited screening through managed inclusion.

Significant shortcomings that I have observed with managed inclusion include problems with the model used to identify passengers for this managed inclusion program and the usefulness of having behavior that takes an officer's implement the managed inclusion program.

The reason I say that, too, Mr. Director, is we have been asking for whatever science that is available relative to behavior detection officers and how that falls into this layered system of protection

and, unfortunately, we have yet to get that report back from a scientific standpoint.

This past Monday, legislation introduced by Subcommittee Chairman Katko, Ranking Member Rice, and me directs TSA to limit expedited airport screening to participants of the PreCheck program and other known low-risk passengers. Our bill passed the House. Last week, three new measures were approved by the Transportation Security Subcommittee.

As we consider the three deals, we know that there are some issues that remain for the full committee's consideration. For instance, significant concerns have been raised by a diverse group of labor stakeholders for the measure aimed to address alarming reports of multiple security breaches caused by employees exploiting security gaps and abusing the credentialing privileges. As we close these gaps, we must ensure that the men and women whose job is to protect the flying public are not unduly impacted.

As TSA legislation works its way through the legislative process, we would welcome constructive engagement from TSA. Administrator Neffenger, again, not only do I look forward to hearing from you on how you plan to address these issues, but also I want to hear from you on how you plan to address the most valuable asset within TSA, which is its workforce.

TSA is plagued with very low morale and an extremely high turnover rate. Employees cite low pay and barriers to advancement as some of their main issues. Additionally, the Federal Air Marshal Service has not had a class in nearly 4 years. Again, I want to know your perspective on this and what steps you plan to take to improve employee morale and if you plan on employing more Federal air marshals.

TSA plays a vital part in protecting America. We can work together to help solve its problems. I look forward to this committee working with you as the new administrator in a bipartisan fashion to help solve TSA's problems and to improve.

With that, Mr. Chair, I yield back.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

JULY 29, 2015

TSA was established by Congress in the wake of the September 11 attacks. It has responsibility for protecting the Nation's surface and aviation transportation systems, and ensuring the free movement of people and goods. Over the years, in protecting aviation systems, TSA has used a number of methods to screen passengers. Some of the technological changes TSA has made, however, have cost taxpayers millions of dollars while failing to adequately address the threat to aviation security.

Unfortunately, TSA is still having problems with its technologies today. For example, last month, it was reported that auditors posing as passengers were able to smuggle mock explosives and banned weapons through checkpoints at various airports across the country. Earlier this spring, the Inspector General released a report claiming that TSA does not properly manage the maintenance of its airport screening equipment. According to the IG, TSA has not issued adequate policies to airports for carrying out maintenance responsibilities.

Administrator Neffenger, I challenge you to address these issues with the technologies used in the airport environment. As you approach this issue, consider both the current threat picture and the emerging threats. Keep in mind that there are small and minority businesses in this country with exceptional technologies that could be beneficial to TSA and improve efficiencies at airports. Former Administrator Pistole implemented a risk-based approach to passenger screening.

However, both the Government Accountability Office and the Office of Inspector General have identified shortcomings with this approach especially when it comes to granting passengers expedited screening through Managed Inclusion. Significant shortcomings include: Problems with the model used to identify passengers for the Managed Inclusion Program and the usefulness of having Behavior Detection Officers implement the Managed Inclusion Program.

This past Monday, legislation introduced by Subcommittee Chairman Katko, Ranking Member Rice, and me directs TSA to limit expedited airport screening to participants of the PreCheck program and other known low-risk passengers. Our bill passed the House. Last week, three new measures were approved by the Transportation Security Subcommittee. As we consider the three bills, we know that there are some issues remaining for the full committee's consideration.

For instance, significant concerns have been raised by a diverse group of labor stakeholders for the measure aimed to address the alarming reports of multiple security breaches caused by employees exploiting security gaps and abusing their credential privileges. As we close these gaps, we must ensure that the men and women whose job it is to protect the flying public are not unduly impacted. As TSA legislation works its way through the legislative process, we would welcome constructive engagement with TSA.

Administrator Neffenger, not only do I look forward to hearing from you on how you plan to address these issues, but also I want to hear from you on how you plan to address TSA's most valuable asset—its workforce. TSA is plagued with very low morale and an extremely high turnover rate. Employees cite low pay and barriers to advancement as some of their main issues. Additionally, the Federal Air Marshal Service has not had a class in nearly 4 years. Administrator Neffenger, I want to know your perspective on this and what steps you plan on taking to improve employee morale and if you plan on employing more FAMS.

TSA plays a vital part of protecting America. We can work together to help solve its problems. I look forward to this committee working with the new administrator in a bipartisan fashion to help TSA improve.

Chairman MCCAUL. I thank the Ranking Member. Other Members are reminded that opening statements may be submitted for the record.

[The statement of Hon. Jackson Lee follows:]

STATEMENT OF HON. SHEILA JACKSON LEE

JULY 29, 2015

Chairman McCaul and Ranking Member Thompson, I thank you both for the opportunity for the full committee to hear from the Department of Homeland Security's new Transportation Security Administrator Vice Admiral Peter V. Neffenger.

As a senior member of the Homeland Security Committee and former Chair of the Subcommittee on Transportation Security, I am pleased to see that the position of TSA administrator has been filled by a person with the credentials and background of Vice Admiral Neffenger.

Vice Admiral Neffenger, I thank and commend you for your decades of service to the Nation.

On April 28, 2015, President Obama nominated Vice Admiral Peter V. Neffenger to be the sixth administrator of the TSA. On June 22, the Senate confirmed Administrator Neffenger to be the administrator of TSA.

Vice Admiral Neffenger was sworn in on July 4, 2015, making him the agency's sixth administrator. Prior to being confirmed to serve as TSA administrator you served as U.S. Coast Guard's 29th vice commandant.

During your time in the Nation's fifth armed service and premier maritime law enforcement agency, you were assigned to several operational and staff roles both domestically and internationally.

This hearing is your first appearance before the committee since you were confirmed by the Senate.

Recently, the Transportation Security Administration (TSA) has faced a number of issues, including detection failure rates, credential misuse, and dismal employee morale.

This opportunity will allow Members to ask you questions about your priorities as TSA administrator, as well as the manner in which you intend to address pressing issues before the agency.

The work of the TSA is a front line Department of Homeland Security and it is not easy—it can in fact be very dangerous.

Like many of my colleagues, I recall the shooting incident at LAX last year that killed Gerardo Hernandez, who became the first TSA Officer killed in the line of duty; and the machete attack at the Louis Armstrong New Orleans International Airport earlier this year that resulted in injuries to Senior Transportation Security Officer Carol Richel.

Vice Admiral Neffenger you are leading an agency that is a critical link in our Nation's first line of defense against terrorism.

As TSA administrator you will lead the primary effort to safeguard transportation throughout the Nation; protect ports of entry from those who would do our Nation harm; fight human trafficking; smuggling; and deter threats too varied for them all to be named.

Each day, TSA processes an average of 1.7 million passengers at more than 450 airports across the Nation.

In 2012, TSA screened 637,582,122 passengers.

The Bush International and the William P. Hobby Airports are essential hubs for domestic and international air travel for Houston and the region:

- Nearly 40 million passengers traveled through Bush International Airport (IAH) and an additional 10 million traveled through William P. Hobby (HOU)
- More than 650 daily departures occur at IAH
- IAH is the 11th busiest airport in the United States for total passenger traffic
- IAH has 12 all-cargo airlines and handles more than 419,205 metric tons of cargo in 2012.

I know that Congress has not done all that it could to make your work easier—Sequestration, a Government shutdown, and a delay in fully funding the Department of Homeland Security was not in the security interest of the Nation.

Recent reports issued by the Government Accountability Office (GAO) and Department of Homeland Security Office of Inspector General (OIG) have identified shortcomings within the agency, raising questions how effectively TSA is fulfilling its mission.

Allegations about mismanagement, wasteful procedures, retaliation against whistleblowers, low morale, and security gaps within the agency are causes for concern.

The DHS IG continues to stress TSA's poor responses to confront problems concerning passenger and baggage screening, access controls to secure areas, and employee misconduct.

The OIG has produced 115 reports on TSA with hundreds of recommendations, many of which remain unresolved.

In addition, to these reports:

- On May 6, 2015, the DHS OIG released a report claiming that TSA does not properly manage the maintenance of its airport screening equipment.
- On June 1, 2015 news media reported on alleged preliminary findings from an on-going undercover DHS Inspector General review.
- Essentially, Red Team auditors posing as passengers smuggled mock explosives and banned weapons through checkpoints at various U.S. airports. According to media reporting, TSA agents failed 67 out of 70 tests or 96 percent of trials. It is important to note that previous Red Teams investigations raised similar concerns. This IG review is still on-going and the report is to be released this fall.

These news reports on premature leaked results from "Red Team" exercises associated with a security at airports were as unfortunate as it was reckless.

The traveling public's confidence in the security of our Nation's airports should not be shaken because of Federal Government planned and managed tests of airport security.

Few people outside of the security field understand how vital the "Red Team" test are to improving security.

"Red Team" test are not a grading system for the day to day work of the Department of Homeland Security's front-line defense personnel.

Red Teams are used to do what we must do if we are to learn how to think like the terrorists and criminals who we must defeat.

We cannot wait until the terrorists figure out a way past security before we act—because this would mean we have learned none of the lessons of September 11, 2001.

We must commit ourselves to do everything possible to prevent another 9/11 from ever occurring again.

For decades Red Teams have been used by the intelligence community and the Department of Defense to seek out ways to overcome security or defense vulnerabilities so that we can learn to build better defenses and make the work of potential attackers harder.

It is a good thing that these tests are conducted because we can learn and develop new security techniques.

I am committed to ending sequestration and making sure that my colleagues in Congress comprehend the gravity of playing politics with security.

I look forward to the testimony of Vice Admiral Neffenger.

Thank you.

Chairman MCCAUL. We are pleased here today to have the new administrator for the TSA. Mr. Peter Neffenger serves as the sixth administrator of the TSA where he leads security operations at more than 450 airports within the United States and a workforce of almost 60,000 employees.

Prior to joining TSA, Administrator Neffenger served as the 29th vice commandant of the United States Coast Guard and the Coast Guard's deputy commandant for operations. We want to thank you for being here today in your debut performance before this committee.

The Chair now recognizes Admiral Neffenger.

STATEMENT OF PETER V. NEFFENGER, ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT HOMELAND SECURITY

Mr. NEFFENGER. Thank you. I have written comments for the record and just a brief opening statement.

Good morning, Chairman McCaul, Ranking Member Thompson, and distinguished Members of the committee. Thanks for the opportunity to testify in my new role as administrator of TSA. I am pleased to appear before you this morning to share my vision and my thoughts about the future of TSA.

Let me begin by saying that TSA is fundamentally a counter-terrorism organization. Our job is to deter, detect, and disrupt those who would harm our system of transportation across the country, especially the aviation sector.

We protect legitimate trade and travel. We have a no-fail mission, one for which the consequences of a successful attack overwhelm the risk equation and for which we must ensure we deliver mission success. This critically important core mission is my highest priority.

As I appear before this committee this morning, I am in the middle of my now fourth week on the job. Although brief, I have been thoroughly impressed with the professionals who occupy our ranks and I want to thank Mr. Thompson for noting those.

Officers and employees who have sworn an oath to serve their Nation in a mission—a critically important mission—that encounters more than 2 million travelers a day in the aviation sector alone. I have also had some time to become more familiar with the challenges facing the agency and develop a set of priorities.

My highest priority is to ensure solutions to the recent covert testing failures. Overall, there are several critical elements that are essential to improving screening operations. First, we must ensure the appropriate measures of effectiveness are in place to drive an institutional focus on our primary mission. What we measure is what our employees will pay attention to. So it is imperative that we get our metrics right.

Second, we must employ a culture of operational evolution, one that constantly reassesses our assumptions, our plans, and our

processes and must be able to rapidly field new concepts of operation and new technologies.

Finally, delivering an effective system in earning the confidence of the traveling public will only come through competence, discipline, performance, and professionalism. I have conveyed these standards to our workforce and I commit to you that I relentlessly pursue these objectives.

I will take on this challenge with the leadership perspective that has been central to my approach my entire career. A well-defined and clear statement of mission, clear and unequivocal standards of performance, training and resourcing that enable the workforce to achieve success in an unwavering pursuit of accountability.

I will set expectations of strong values for the workforce and I will lead with TSA's core values of integrity, innovation, and team spirit at my core.

Since its creation after the attacks of September 11, 2001, TSA has played an invaluable role in protecting the traveling public. However, nearly 14 years later, we continue to face a range of threats from terrorists who are inspired by messages of hatred and violence. A number of terrorist groups remain intent on striking the United States and the West, and we know that some of them are specifically focused on aviation.

More troubling, today the threat is more decentralized, it is more diffuse and more complex than ever before. These persistent threats are TSA's most pressing challenge. Our enemies will continually adapt and so must we. We must leverage intelligence, technology, the experience of our front-line operators and our partners in Federal, State, and local governments in the private sector, to employ effective measures. We must pay particular attention to the insider threat.

A second challenge facing TSA is retention, training, and accountability. Front-line managers and screeners are critical to our success. Agency culture, morale, and effectiveness are a direct result of career-long development recognition and accountability.

The traveling public expects to be treated with dignity and respect. I will pay close attention to training and workforce development to include how to leverage and expand the TSA academy to develop leaders, improve individual performance, and instill a greater sense of pride in our agency, its mission, and its values.

A third organizational challenge for TSA is to ensure it is continually fielding the tools and equipment the workforce needs today, while envisioning how to modernize our system and transform the traveling experience in the future. I see a future where advanced capabilities can transform the experience, while preserving risk-based security as a central feature.

I think it is possible that an individual's biometric identity could effectively become the boarding pass of the future, linked to intelligence systems and requiring passage through an integrated capability designed to detect metallic- and non-metallic-based threats. This future can be realized with a suitable strategic approach.

As such, I commit myself to ensuring that TSA remains a high-performing, highly-capable counterterrorism organization, guided by a risk-based strategy, employing a multi-layered, intelligence-driven operation, and that we recruit and retain a highly-trained

workforce, one that has the opportunity for career growth and development, while placing a premium on professional values and accountability; that we pursue advanced capabilities with innovation and competition central to our way of thinking, and that TSA continues to strengthen its integration in the intelligence community, in the private sector with our stakeholders, and among DHS and other Federal, State, and local partners.

I will follow this strategy, develop and lead the workforce, adapt and invest appropriately, and remain focused on these critical success factors.

Then finally, throughout my years of service, I know and I remain aware of the need to balance desires for greater security, with protection of the liberties and the rights that we cherish. Safeguarding civil liberties and privacy interests is a top priority, and I look forward to partnering with this committee to enhance the safety of the traveling public, and to achieve this balance.

I applaud the work that the men and women of TSA perform each and every day. It is a great honor to join them, and to have the privilege of serving with them in the defense of our country. Chairman McCaul, Ranking Member Thompson, and Members of the committee, I thank you for the opportunity to be here today, and I look forward to your questions.

[The prepared statement of Mr. Neffenger follows:]

PREPARED STATEMENT OF PETER V. NEFFENGER

JULY 29, 2015

Good morning Chairman McCaul, Ranking Member Thompson, and distinguished Members of the committee. Thank you for the opportunity to testify in my new role as administrator of the Transportation Security Administration (TSA).

It has been my privilege to serve our Nation for the past 34 years in the United States Coast Guard. Throughout my career I have worked to advance my agency's mission while maintaining a deep sense of accountability to the American people who entrust us with their protection. I look forward to carrying these efforts forward as I undertake my responsibilities as TSA administrator.

I am especially honored and privileged to work with the men and women of TSA. Our front-line workforce carries out an incredibly difficult and demanding mission of protecting our Nation's transportation systems and ensuring freedom of movement for people and commerce. To be clear, this is a difficult job and our employees work diligently to secure transportation systems for our Nation. I respect and appreciate our TSA employees who rise to the challenge on a daily basis.

The work of TSA employees covers a wide array of duties, ranging from intelligence-based screening, to physical screening, to monitoring and inspections. In fiscal year 2014, Transportation Security Officers (TSO) screened approximately 660 million passengers and nearly 2 billion carry-on and checked bags. Our officers prevented 181,000 dangerous, prohibited items, including 2,200 firearms, from being carried onto planes. They screened a daily average of 6 million air passengers against the U.S. Government's Terrorist Screening Database; routinely prevented known or suspected terrorists from boarding aircraft; and conducted enhanced screening of passengers, as necessary, prior to boarding an aircraft. In addition, TSA's Federal Air Marshals protected thousands of flights. Transportation Security Inspectors completed over 1,054 airport inspections, 17,894 aircraft operator inspections, and 2,959 foreign air carrier inspections to ensure compliance with rules and regulations.

TSA faces unique challenges in its efforts to protect our Nation's transportation systems. While intelligence shows us we must remain focused on aviation security in particular, TSA is also charged with securing mass transit, rail, highway, and pipeline sectors. To function effectively, TSA must continue to develop in its role as a counterterrorism agency with a dedicated and professional workforce. We must strengthen the security of our transportation systems, using an array of capabilities

including intelligence information, technology, and most importantly, the dedication and vigilance of every employee at TSA.

More than a decade after the terrorist attacks of September 11, 2001, today's terrorist threat is more decentralized, more diffuse, and more complex. Today's terrorists publish their instruction manuals on-line and call on their followers to take action. The persistence of this more dispersed threat is among TSA's most pressing challenges. Our enemies will continually adapt, and so must we. TSA must leverage intelligence, technology, and the experience of our front-line operators and private sector partners to ensure we employ effective, efficient, and ever-evolving procedures to stop those who would harm us.

Given the threat and enormous challenge accompanying the task at hand, I recognize the importance of being a strong leader for TSA—one who will explore new ideas and reevaluate current procedures to ensure we have the appropriate security in place to protect the traveling public. I am honored by the President's trust in me and I sincerely look forward to serving in this important leadership position.

AGENCY PRIORITIES

The critically important core mission of TSA is to secure the Nation's transportation systems and the people who use those systems. This is my highest priority. To this end, I have a three-fold approach: Employing a strategic, risk-based methodology; developing, training, and leading a capable workforce; and pursuing advanced and effective security capabilities.

First, a strategic, risk-based approach to protecting transportation is critical given the rapidly-evolving global terror threat and persistent adversaries who continually adapt their methods and plans for attack. TSA must leverage the latest intelligence to inform operations and investments. We must employ risk-based operations tailored to each operating environment and transportation mode, not one-size-fits-all solutions. To be successful in this endeavor, I intend to incorporate intelligence to inform our strategy and operations, as well as to expand and strengthen TSA's existing partnerships with stakeholders for greater information sharing and unity of effort.

Second, we are also mindful of our interactions with millions of travelers each day, and to that end, must place an emphasis on professionalism and accountability while we recruit and retain a skilled and highly-trained workforce. Further, our officers must be constantly trained, developed, and supported in their efforts. This training should incorporate the ideas of a culture of adaptation, where our workforce constantly questions assumptions, plans, and processes, and is able to adapt to new operating procedures, standards, and capabilities. Our workforce must be highly capable and well-trained, with a strong career path for growth and development. Effectiveness is a direct result of consistent training, recognition, and accountability. As such, my expectations for the workforce include a strong emphasis on values, high standards of performance, and accountability. The traveling public expects efficient and effective screening, and to be treated with dignity and respect. We must continually reinforce this message of dignity and respect in training for the front-line workforce and management alike to ingrain these principles into agency culture. Delivering an effective security system requires that we have the confidence of the traveling public; we earn that through competence, disciplined performance, and professionalism.

Finally, TSA must pursue advanced and effective capabilities in the development, acquisition, and deployment of our technology, as well as our strategies for checkpoint screening procedures. We must employ a strategic systems-focused approach to ensure we are evolving in our capabilities and ability to detect and disrupt the latest threat streams. We will leverage our team's experience in acquisition and innovative sourcing to lead TSA in the next phase of the agency's development. This focus will help TSA to invest its resources to systemically reduce vulnerabilities and mitigate risks.

IMPROVING SCREENING OPERATIONS

TSA faces a number of challenges, which I plan to address by evaluating screening operations and meeting the standards the American people expect. First among these efforts will be addressing the recent covert testing of TSA's checkpoint operations and technology conducted by the Department of Homeland Security (DHS) Office of Inspector General (OIG). I am greatly disturbed by TSA's failure rate on these tests, and have held numerous briefings and meetings to better understand the nature of the failures, the root causes, and the scope of the corrective actions needed. I am committed to working with senior leaders at TSA and DHS to formu-

late solutions that will enhance our effectiveness at checkpoint operations—and then to test those enhancements.

To that end, I am carrying out DHS Secretary Johnson's ten-step plan as follows:

- Brief all Federal Security Directors at airports Nation-wide on the OIG's preliminary test results. This was completed in May.
- Train every TSO to address the specific vulnerabilities identified by the OIG tests. We are now implementing this in a phased approach, which began May 29, 2015 and is to be completed by the end of September 2015.
- Increase manual screening measures, including reintroducing hand-held metal detectors to resolve alarms at the checkpoint. This has been underway since mid-June.
- Increase use of random explosives trace detection, also started in mid-June.
- Test and evaluate screening equipment to measure current performance standards.
- Assess areas where screening technology equipment can be enhanced.
- Evaluate the current practice of including non-vetted populations in expedited screening.
- Revise TSA's standard operating procedures to include using TSA supervisors to help resolve situations at security checkpoints. On June 26, 2015, TSA began field testing new standard operating procedures at six airports. Lessons learned will be incorporated and deployed Nation-wide.
- Continue covert testing to assess the effectiveness of these new actions. For each test, there must be a same-day debrief with the workforce of what did or did not work along with immediate remediation actions.
- We have responded vigorously to establish a team of TSA and other DHS officials to monitor implementation of these measures and report to the Secretary and administrator every 2 weeks.

While these immediate actions address specific vulnerabilities identified by the OIG tests, our systemic review over the coming weeks to identify vulnerabilities across the aviation security system will be invaluable. The assessments are designed to determine the proximate root causes of these failures and provide effective system-wide solutions.

RESPONDING TO THE INSIDER THREAT

The December 2014 incident involving an alleged gun smuggling ring at Hartsfield-Jackson Atlanta International Airport highlighted the potential for airport and airline employees to use their access for illicit purposes. In January 2015, Secretary Johnson and TSA consulted the Aviation Security Advisory Committee (ASAC) to review the issues associated with insider threats and asked for their recommendations to improve airport employee access control at our Nation's airports. The ASAC completed its 90-day review in April of this year, and delivered its 28 recommendations to TSA.

TSA immediately implemented five initial action items recommended by the ASAC, which include: A requirement for airports and airlines to conduct fingerprint-based Criminal History Records Checks (CHRC) every 2 years for all airport and airline employee badge holders until an automated recurrent vetting solution is complete; a reinforcement of existing requirements that employees traveling as passengers be screened by TSA; a reduction in the number of access points to secured areas to an operational minimum; increased random employee screening; and a joint effort with our stakeholder partners to leverage the DHS "If You See Something, Say Something™" initiative to encourage reporting of insider threat activity.

In addition to those immediate steps, we began a phased implementation of the Federal Bureau of Investigation (FBI) criminal history monitoring program, Rap Back, with an aviation pilot beginning at Dallas Fort Worth International Airport and Boston Logan International Airport, and with Delta Air Lines. The program ensures real-time criminal history monitoring of the aviation worker population. Rap Back is part of the FBI's Next Generation Identification Program, introduced in September 2014.

TSA fully concurs with 26 and partially concurs with the other two recommendations of the ASAC report. Statutory limitations in one instance and the need to conduct a detailed cost-benefit analysis locally in another are the reasons for the partial acceptance of two recommendations.

We are acting on the ASAC recommendations and have set a definitive schedule for assessing and reporting the results on actions taken based on the recommendations.

ADVANCING RISK-BASED SECURITY (RBS) AND EXPEDITED SCREENING

I am a strong proponent of a risk-based approach to security. The vast majority of people, goods, and services moving through our transportation systems are legitimate and pose minimal risk. The first necessary effort in pursuing risk-based security is to identify the low-risk majority so that we are not forced to apply our scarce resource capabilities to known or unknown threats. The drawbacks of a single approach are clear—severely limiting effectiveness and efficiency while perhaps introducing vulnerabilities and opportunities for harm. If we can understand the threats and identify the vulnerabilities of our systems, then we can design our security system to reduce the risk and close vulnerabilities.

I hear and understand the concerns raised by this committee and the OIG about the current application of TSA's Risk-Based Strategy (RBS) approach. Expedited screening should be available to fully-vetted populations. We are reviewing the procedures for expedited screening and an evaluation of the appropriateness and effectiveness of the various security tools currently in use.

I am committed to refining and enhancing our expedited screening procedures, including TSA PreCheck™. One of the major ways for us to expand the number of known and trusted travelers eligible for expedited screening will be through the expansion of the TSA PreCheck™ Application Program. I look forward to efforts such as expanding participation to additional U.S. and foreign airlines, exploring potential opportunities to leverage private-sector capabilities and expertise in the TSA PreCheck™ application process, and offering additional opportunities for enrollment in TSA PreCheck™ to increase the number of vetted enrollees. These opportunities present important opportunities for changing the dynamic of checkpoint screening Nation-wide, and most importantly present us with an opportunity to focus on those passengers about whom we are most concerned—or those about whom we know less—to ensure maximum security for the traveling public. These efforts will make entry into the aviation security system for those who are interested in sharing more about themselves more accessible and available. The goal is to move towards a known and vetted population.

CONCLUSION

Chairman McCaul, Ranking Member Thompson, 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.

Chairman MCCAUL. Thank you, Admiral. I now recognize myself for questions.

Admiral, as you and I know, al-Qaeda, particularly al-Qaeda and the Arabian Peninsula, and the Khorasan Group in Syria, are still very intent on hitting the aviation sector, primarily through bombs, specifically non-metallic IEDs. This led to a heightening of screening at 25 airports overseas.

We have made some progress against them through strikes, recently taking out the leader of the Khorasan Group, and others. But that threat is still there. With this dismal report card that came in, 96 percent failure rate.

Given the threat that is out there, I am concerned about the safety of the American people when they travel on airplanes; not to mention that 73 aviation workers have potential ties to terrorism.

Now, I can't get into all the details, because it still remains Classified in terms of what slipped through the cracks. But what are you doing—what are you planning to do as the new TSA administrator to address this enormous failure?

Mr. NEFFENGER. Mr. Chairman, thank you for the question. You are absolutely correct to point out that this is a huge concern, and it greatly disturbs me to know that we had that failure rate at the checkpoint.

As you know, the checkpoint, although not the only element in our system of security, is a critically important element in the sys-

tem of security. It is the barrier between the sterile and non-sterile areas of an airport. It is a visible deterrent, and it is a last chance to catch items that we do not want getting on-board aircraft.

So as I looked at the failure rate, my immediate questions were the same ones that Secretary Johnson had. As you know, that came out during my nomination and confirmation process, and I had a number of conversations with the Secretary. He immediately ordered an establishment of a team to take a hard look at the nature of the failures and what they have done.

So I have inherited that team. I have seen the work that they have done. What I can do, is I will speak directly to what that team is doing, but then I will speak in more systemic terms of what I think it is telling us about where our concerns are.

As you know, I will begin by saying that covert testing is a net-positive because you want to try to break your system of security on a daily basis to ensure that you have got it right. It goes back to the need to continually adapt and evolve your organization. But when it breaks to the extent that we saw, that raises some significant questions about how effective you have been.

So what the team has done, is they took a hard look at exactly what the nature of each individual failure was. We looked case by case of the tests that the I.G. did. The I.G.—and I have sat and talked with the I.G. extensively about this, and they have been quite open about sharing their results.

We looked at the nature of the test, and we looked to see, is it a technology issue, is it a human-performance issue, is it a process or procedure issue? As you might suspect, it is, in some cases, some combination of those three elements.

Then we looked to see whether there was a way to mitigate that, so that what the team has done over the past 3 months is to take apart all of those. They have got a detailed brief. I would offer to the committee a detailed brief on the specifics of that team. I think it would be—it would help you to understand how we are moving forward.

Then we looked at, how do we train out those specific failures? Because the immediate need is to train out those failures so that we don't have a repeat of those. We are now in the process of doing that. Over the course of the next 60 days, by the end of September, we will have trained the failure, the specifics about the failures, to every front-line member of TSA.

That will address the immediate problem. I think that we can do that. The bigger question is: Are there systemic issues in the way we are approaching our business, that led to those failures in the first place, so that we—what I don't want to see is some other set of failures in the future.

I know that I can train to these, but I am interested in figuring out how we train to the larger, and to the larger questions out there. That is what we are working on now. That goes to a vision for how you then begin to think of yourself in this continuously-evolving, continuously-adapting way.

As I said, the thing to remember is that there are other elements of the system; some of them virtual, some other physical elements of the system. But the checkpoint is one of the most important, and we have to get that right.

Chairman MCCAUL. You talk about technology and vision for the future—you and I have talked about this privately—it seems like we have—you know, PreCheck I think has been a success in global entry, makes more passenger-friendly, more risk-based, which I think is where TSA should go.

But as we look at the future, the checkpoint of the future, and the use of technologies, what is your vision for the next, say, 5 to 10 years? What will the experience be like? What is your goal for the traveling passenger?

Mr. NEFFENGER. That is a wonderful question, because as somebody who has traveled a lot over the years, I know what checkpoints can feel like when you get there. I do think that there is a vision for something in the future.

One of the best terms I have heard recently was "security at the speed of life." I like that. There are a number of interesting and innovative ideas out there.

I mentioned one in my opening statement; the idea that you are your boarding pass. If I can tie you biometrically to a reservation, to an identification, and I can do so in a verified way, then, one, that moves you through the process faster. We eliminate boarding passes.

As you know, every airline has a different style of boarding pass. It makes it very challenging for those document checkers to check those, because they are looking at something different. There is not a lot of consistency there.

So I think we can eliminate the boarding pass. I think we can move to integrated technology that does—and right now there is a challenge because the AIT machines don't do metal detection. Metal detectors don't do non-metallic explosives. Nothing sniffs for explosives as you go through. I have actually seen prototypes of machines that you can walk through, and it does all of that in one.

Now, can they be fielded effectively? I don't know. I think this goes back to your earlier question about competition. I think we could do a lot more to incentivize competition in the private sector.

I am currently right now tied to a process that has me buying a lot of equipment that may be obsolete shortly after I buy it. I have to adapt continuously to a changing threat. I look at the way the Department of Defense, for example, has periodically incentivized competition in the private sector to come up with new ideas.

I think there are ways to do that. I would love to have more conversations with this committee on ways that we can do that, ways that we can use or modify some of our acquisition practices and policies to allow us to do that.

Chairman MCCAUL. Well, I will look forward to working with you on that. Thank you for your testimony. The Chair recognizes the Ranking Member.

Mr. THOMPSON. Thank you very much. Mr. Neffenger, your comments, clearly, a breath of fresh air. I think the Chairman will agree with me on that.

We have passed a modernization of acquisition legislation to kind of give the Department a freer reign. One of the challenges we have is the culture of, "But we have always done it this way."

So we buy technology, being TSA, that we already know does not address the emerging threat, but because, "This is how we do." Members of Congress have raised that question a number of times.

I am glad to see you willing to say, "How can we get out of this?" CIA, NASA, some of the other agencies, they have vehicles that they use to incentivize the acquisition of new technology. Some of it is you create a venture for them, and you purchase participation with those companies so they can continue the development.

We tried that for quite a while. I want to talk to you a little bit about that going forward. But as we talk about technology, let's talk about how we do processing. The Managed Inclusion program, some of us have had real problems with it.

It appears that the issue became, "How can we get people through the checkpoint faster?" rather than, "How can we guarantee that those people who go through have actually been vetted?" So we had cross-purposes.

How do you see the Department working on this Managed Inclusion program?

Mr. NEFFENGER. Well, thanks for your question.

I agree completely with you. I would like to see us, and in fact I have ordered a phasing out of the Managed Inclusion Program, because I think—the goal is to have a fully-vetted population in the PreCheck Program. The more I know—I want known people, people I trust going through the program.

That is really the heart of risk-based security is I want to separate a known population from the ones I don't know anything about, I want to make the experience less intrusive for the known population, one that reduces the burden on the agency. I am paying attention to the things I need to pay attention to versus people that have already vetted.

So, I think we have to phase out Managed Inclusion, because it introduces, I think, perhaps a higher level of risk than we want in the system. I want to grow the use of passenger-detecting—I mean, passenger-screening canines. These are the explosive detection dogs that we have out there. That is a—I mean, they are a tremendous asset and we are looking to expand that program slightly and to reposition some of the K9 teams that we have in locations that are lower-risk to higher-risk locations.

But more importantly, I want to look to—we are working on a request for a proposal to put out the option for private-sector third-party screeners to help us do the initial marketing and collection of people into the PreCheck Program. I have had a number of conversations with travel aggregators, with credit card companies and the like, and I think that there is an opportunity to expand that PreCheck population, the known population, enrolled population over the near term, and so I am encouraged by the opportunity.

I am hoping that this request for proposal generates a lot of interest and competition in in the private sector, and then to grow that population, but that is my move. Then to move people that are already screened, like we did with military members and others, that have already had background checks, that have already biometric on file, into the PreCheck Program based upon their ongoing clearances.

Mr. THOMPSON. A couple other questions.

One is the whole employee morale issue. Every OPM report that we read lists DHS at the bottom, and more specifically, TSA. How do you plan to get us off the bottom?

Mr. NEFFENGER. Well, I read the Federal employee viewpoint survey that TSA did, and you are right, it doesn't rank near the top of organizations. I think, as I go back to what I said in my opening statement. I think morale is a—first of all, it starts with a clear understanding of mission.

Actually I start with the fact that every one of them raised their hand and took an oath of office to support and defend the Constitution of the United States. That is a huge statement. If you think about it, how few people in this country do that? So they took a job that—I am sure their eyes were open, they knew it wasn't the most popular job in the country. But they said, "I want to be the face of security for the traveling public." That is where morale starts.

Now, where does morale fail after that? It is when—it is if there is a disconnect between what they think they signed up for and what they think the organization is asking them to do.

So, I go right back to mission, and my three decades in Coast Guard taught me that it starts with mission, and then you have to talk about that mission, and you have to train to that mission, and you have to measure that mission. So if I come to work, I want to know that I am—that my agency is not only giving me the tools and the training I need to do it, they are doing it on a regular basis, and they are backing me up when I have to make decisions.

So, I think there is a lot of training of that, and I think that there is a work force engagement piece.

Mr. THOMPSON. Thank you.

My last question, Mr. Administrator, with respect to the TWIC card. We have resolved the problem, with this committee's help, that people who applied don't have to go back. Now we are hearing that when they try to get re-certified, there is a tremendous backlog, so that members' TWIC card expires before the new card comes, and we would like for you to look at that.

So, in this committee's efforts, I don't want us to have created a bigger problem by alleviating the second trip, and we didn't fix the getting the TWIC card back to the person.

The last item is, those TWIC card workers who work on military installations on selected instances are being required to get an additional card, it costs about $200, that asks the same information that the TWIC card asks. So, can we see if there is some reciprocity that the TWIC card can provide to other installations, so that those workers don't have to pay for a second card?

Mr. NEFFENGER. Well, I am not familiar with the concern that you are raising, but if I can get with your staff to find out what that issue is, I will certainly look into that. I think it would make sense if we can—if we are collecting the same information, we can verify the same things, then I think it makes sense to work on reciprocity.

Mr. THOMPSON. The issue of getting the cards back before they expire?

Mr. NEFFENGER. Yes, sir. Again, let me find out what our current backlog is. I know that the TWIC has been a challenge over the

years, and it is a focus area for me as I move forward. I would like to know what the backlog is and again, are there things that we can do that can dramatically speed up that process?

Mr. THOMPSON. Thank you very much.

I yield back.

Chairman MCCAUL. Mr. Rogers is recognized.

Mr. ROGERS. Thank you, Mr. Chairman.

Admiral, welcome. You have got a big challenge on your hands. I have been on this committee since it was established, I have seen the Department grow and develop since it was established, and I can just assure you you have some inertia to deal with. You have some employees that you are gonna have to put the fear of God in their heart or nothing is going to change.

I have seen some good administrators precede you that ran into administrative pressures to back off; you are gonna run into that. But I want you to understand that you have got some folks that really believe they don't have to change, you will be gone before they are, and you need to make them understand that is not the case.

If they don't change what they are doing—now, it can't be slight changes, it is gonna be dramatic changes, or we are gonna have the results we have been getting for the last several years.

This most recent I.G. report that upset so many people was identical to the previous three I.G. reports over roughly a 5-year period of time. That is unacceptable, and that is people who are unwilling to do anything different and don't believe there are consequences for not doing anything different.

So, I hope that you will instill that understanding in them, that if they don't change, they are gone, and if you can't do that, you ought to be gone, and I think you would agree with that.

One concern I have got, I heard the Chairman make reference to the PreCheck program. Very good program as far as its goals. The problem we are running into, and I think when you move around airports you will see this, is that frequent travelers who are the people we want into this program, have gotten in to it. The FSDs at the airports have not adjusted the lane activity to accommodate that traffic, so now you spend more time in the PreCheck line than you do if you go into the priority lane—sky priority, whatever they call it, and just go through the typical take-your-shoes-off type.

That is silly, people are gonna stop going into the PreCheck program if they don't it find it enhances their ability to get through in a faster fashion. So, I hope you will address that issue with these airport folks, because we want the PreCheck program to continue and to be the method of getting safe people that we know through in an efficient manner so we can put more attention on those infrequent travelers who are more apt to have a problem.

I did hear you make reference to the fact that you understand the explosive detection canines are a valuable asset. They are the best asset you have, and I am not gonna talk in a open setting about the efficacy of the equipment or the personnel, but I would like to, soon as we are back from our August district work period, to meet with you in the SCIF and go over in detail what the shortcomings have been.

I used to chair the Transportation Security Subcommittee, I am very familiar with this subject matter and what I think needs to be done to remedy that. So, I look forward to that and I hope I can get your commitment to meet with me in September for that purpose.

Mr. NEFFENGER. Yes, sir, I would be happy to do so.

Mr. ROGERS. That is all I have got. Thank you, Mr. Chairman, I yield back.

Chairman MCCAUL. Gentleman Chair recognizes Ms. Jackson Lee.

Ms. JACKSON LEE. First, let me offer my appreciation to my Chairman and Ranking Member for your presence here today, Vice Admiral, and let me thank you for your service. It is interesting that I followed my good friend Mr. Rogers, because as he chaired, I think we have switched back and forth. I had the privilege of chairing the Transportation Security Committee, and service—and I think I have served as his Ranking when he was Chair, and we are, if you will, young but we have been here for a little bit.

So we are really grateful for you service, and again, that of my Chair and Ranking Member of the full committee.

Let me, as I thank you for service, let me take a different twist and say to you that I am very proud of the men and women who serve every day on the front lines in many ways, but in particular today of transportation security officers.

Over the years, I have argued for increased professional development training, to recognize that morale and commitment have a lot to do with pay, respect, and professional development training, and I am gonna be posing questions within the short period of time that I have.

Let me also acknowledge to my colleagues, again, my sympathy to the Hernandez family for Mr. Gerardo Hernandez killed in the line of duty as a Transportation Security Officer in Los Angeles. Some of us went out to Los Angeles to acknowledge that as well as meeting with his family.

We should never dismiss the fact, in all of the issues that you will have to deal with, is that since 9/11, there are probably millions of TSA screenings, TSO screenings, and any number of stops that the TSO Officers made—and I hope you acknowledge that, because beginning to correct starts with acknowledging service, and I think it is very important to do so.

Let me also say, however, that in addition to that, we have allegations of mismanagement, wasteful procedures, retaliation against whistle blowers, low morale, security gaps. We have a number of things that you will have to address, but I never want to leave this table without saying thank you to the TSO Officers.

I make it my business, as I travel in airports across America, to say hello, to ask a question, or to watch their procedures, and again if I might, professional development training is crucial.

So let me just ask you a series of questions that I hope I will be able to get in. One, I think you can do better if we all get rid of sequestration. I want to get that on the record because you need the money placed in the right places.

I agree with the use of privatization on the basis of—let me correct that for being misquoted. I believe there is a place for the pri-

vate sector in particular dealing with technology. I might have misheard you when you said something about a third TSA and it was the private sector. So I hope that is not right.

I am against privatizing airports and privatizing TSO Officers. I think we need a professional, trained group. I want your comments as it relates to professional, trained groups.

But on the BDO, there is $700 million being spent on that. I would be interested in you being able to craft an effective utilization of these individuals or this project with a more effective use of the resources that you are given on that, also BDO.

I want to take note of the fact that a young man in Dallas was so in love with his girlfriend just recently ran past security. I would like your comment on that. We shut down the Newark Airport a couple of years ago with another enamored young man who went through security.

Then I would like to have your comment that TSOs are the most visible face of security in America. How do we make people run toward, meaning the good people, and say I am so happy, as most people do, about these issues?

If I might yield to you for these answers. Again, I hope I can join Mr. Rogers and others for that SCIF briefing. I would be happy to do so.

If you could just comment on those, I would greatly appreciate it.

Mr. NEFFENGER. Thank you, Congresswoman Jackson Lee. Thank you, first and foremost, for acknowledging the workforce. I couldn't agree with you more. The mission of TSA is delivered by those front-line transportation security officers across this Nation.

I can't say enough how important they are to the success of the program, but I can't also thank them enough for the work that they do. I intend to do that and I do that myself whenever I travel and certainly now.

With respect to budget, I think you are right, sequestration is going to be a challenge for every Government agency that will be subjected to it. I hope that the Congress is able to pass a budget resolution that will eliminate sequestration and allow us to have some certainty going forward.

To correct, to make sure it was clear what I was saying with respect to third party, I was really speaking about incentivizing private-sector entities, private-sector businesses to help develop the technologies we need into the future.

I think that there is a way to do that in a competitive way, in a competitive environment, and to provide incentives that don't have governments taking on all the risks to development, don't have Government buying, you know, huge capital outlays for equipment that then later becomes obsolete.

The BDO program, as you know there has been some controversy about that program. There have been a number of GAO audits and one I.G. audit that has looked at the efficacy of the program and the work that is done.

I know that TSA contracted out a third-party overview of that program. That third party spent 2 years collecting data on that program and running tests. That was submitted in the report.

Then there is a question with respect to the underlying concerns. I know that we are in the process of completing a report showing what we believe to be the scientific underpinnings of that.

That said, I understand the concern with the use of that. From my perspective, and I am not clear on how I feel about the BDO program yet, being relatively new, but from my perspective, if I can show a link to validated, scientific underpinnings, if I can show some effectiveness with behavioral viewing, then I think that it is a good tool to have in the security toolkit.

I know that law enforcement agencies around the world use behavioral indications as a way of determining if they have got problems, whether you are a beat cop or you are looking at other situations.

So I think that I am looking forward to reading that report that was done that looked at the scientific underpinnings, and then I look forward to discussing that further with the committee.

The security breach at Dallas Airport that you mentioned, that is of great concern to me for a couple of reasons. One, I am very concerned about the safety of our front-line workforce. Officer Hernandez, a tragic loss of Officer Hernandez, the attack in New Orleans earlier this spring, those are very real threats that can face our front-line workforce and you have to be careful of that.

So any potential for somebody to breach a barrier runs the potential for not just a safety issue, but obviously the security issue.

So I ordered an immediate review of that incident. I want to find out what happened. But more importantly, again, this goes back to the systemic issue, you know, I don't want to just go around whacking every one-off problem that exists. I want to look at the system and understand, do we have an issue with security at our checkpoints? Again, that is the barrier between the non-sterile and the sterile areas. There has to be an expectation of that barrier working.

So I don't have the full results of the investigation of that yet. I will share that with you when I have it. But more importantly, I am going to look across the system and look at how we are doing this.

Ms. JACKSON LEE. Thank you for your courtesy.

May I put this in the record, please, Mr. Chairman?

Chairman MCCAUL. Yes, without objection.

Ms. JACKSON LEE. Thank you.

Chairman MCCAUL. Do you want to state what it is?

Ms. JACKSON LEE. "Undercover DHS test finds security failures at U.S. airports." I would just like to put this in the record so we can discuss it further. Thank you.

Chairman MCCAUL. Without objection, so ordered.

Ms. JACKSON LEE. Ask unanimous consent. Thank you.

[The information follows:]

ARTICLE SUBMITTED FOR THE RECORD BY HON. SHEILA JACKSON LEE

UNDERCOVER DHS TESTS FIND SECURITY FAILURES AT U.S. AIRPORTS

Jun 1, 2015, 7:04 AM ET

By Justin Fishel, Pierre Thomas, Mike Levine, and Jack Date via Good Morning America

An internal investigation of the Transportation Security Administration revealed security failures at dozens of the Nation's busiest airports, where undercover investigators were able to smuggle mock explosives or banned weapons through checkpoints in 95 percent of trials, ABC News has learned.

The series of tests were conducted by Homeland Security Red Teams who pose as passengers, setting out to beat the system.

According to officials briefed on the results of a recent Homeland Security Inspector General's report, TSA agents failed 67 out of 70 tests, with Red Team members repeatedly able to get potential weapons through checkpoints.

In one test an undercover agent was stopped after setting off an alarm at a magnetometer, but TSA screeners failed to detect a fake explosive device that was taped to his back during a follow-on pat down.

Officials would not divulge the exact time period of the testing other than to say it concluded recently.

Homeland Security Secretary Jeh Johnson was apparently so frustrated by the findings he sought a detailed briefing on them last week at TSA headquarters in Arlington, Virginia, according to sources. U.S. officials insisted changes have already been made at airports to address vulnerabilities identified by the latest tests.

"Upon learning the initial findings of the Office of Inspector General's report, Secretary Johnson immediately directed TSA to implement a series of actions, several of which are now in place, to address the issues raised in the report," the DHS said in a written statement to ABC News.

Homeland security officials insist that security at the Nation's airports is strong—that there are layers of security including bomb-sniffing dogs and other technologies seen and unseen. But the officials that ABC News spoke to admit these were disappointing results.

This is not the first time the TSA has had trouble spotting Red Team agents. A similar episode played out in 2013, when an undercover investigator with a fake bomb hidden on his body passed through a metal detector, went through a pat-down at New Jersey's Newark Liberty Airport, and was never caught.

At the time, the TSA said Red Team tests occurred weekly all over the United States and were meant to "push the boundaries of our people, processes, and technology."

"We know that the adversary innovates and we have to push ourselves to capacity in order to remain one step ahead," a TSA official wrote on the agency's blog in March 2013. "[O]ur testers often make these covert tests as difficult as possible."

In a 2013 hearing on Capitol Hill, then-TSA administrator John Pistole, described the Red Team as "super terrorists," who know precisely which weaknesses to exploit.

"[Testers] know exactly what our protocols are. They can create and devise and conceal items that . . . not even the best terrorists would be able to do," Pistole told lawmakers at a House hearing.

More recently, the DHS inspector general's office concluded a series of undercover tests targeting checked baggage screening at airports across the country.

That review found "vulnerabilities" throughout the system, attributing them to human error and technological failures, according to a 3-paragraph summary of the review released in September.

In addition, the review determined that despite spending $540 million for checked baggage screening equipment and another $11 million for training since a previous review in 2009, the TSA failed to make any noticeable improvements in that time.

Chairman MCCAUL. Mr. Katko is recognized.

Mr. KATKO. Thank you, Mr. Chairman.

I want to first of all echo the sentiments of Mr. Thompson that you are indeed a breath of fresh air. We have spent a lot of time together in the last few days and since you have come on-board and I think you are exactly what TSA needs at this time.

I also echo the sentiments of Mr. Rogers that there are a lot of problems at TSA. But I also—I sound like a politician—but I also echo the sentiments of Ms. Jackson Lee and want to say thank you for the good work that the vast majority of your employees are doing day-in and day-out. You are often trying to find a needle in the haystack and I appreciate the efforts of everyone.

One of the areas I want to focus on a little bit today is the issue of access control. We have kind of touched on it, but I think it is a gaping hole in security at the airports Nation-wide.

Within the last year or 2, you have had a major drug trafficking ring operating out of the Oakland Airport. You had another one operating out of Dallas/Fort Worth Airport that has truly troubling implications based on the briefings I have received so far about it that aren't necessarily public.

Another one, of course, that is very troubling was an individual who smuggled as much as 160 guns, loaded, including assault rifles, on airlines because a worker at the Atlanta Airport carried the guns in bags through the access points and brought them up to New York City. At any point, instead of selling them, if he wanted to do something bad on an airplane we would have had an unbelievable tragedy on our hands.

I think these incidents point out that there really is a major problem with access controls at airports. I recently had a bill passed out of our committee, our subcommittee addressing the issue.

But I would like to hear your thoughts on the access control issue. Should there be minimum standards at all access points of these airports?

I will preface the question further by saying that it is clear from the Dallas case that the VIPR teams that are used to do the random screening at various points were being monitored by the bad guys at Dallas/Fort Worth and they were just simply avoiding them with a quick phone call to their colleagues.

So that is not going to work going forward. So with that overview and those set of prefaces, I would like to hear your thoughts on access controls.

Mr. NEFFENGER. Thanks. I agree with your concern. As you know, those incidents—let me back up a little bit and talk in general terms. This should be a known and trusted population. Every one of these workers gets vetted for background. There is a question as to how far we need to go back in the future, but that we vet them for background, they are continuously vetted, any credential holder is continuously vetted against the terror screening database.

Then currently, there is a periodic revetting against criminal databases. That doesn't guarantee that you don't have a criminal population, that just guarantees that they didn't show up at that point.

So what do you do about the potential for criminal activity or worse in a known and trusted population? You introduce uncertainty in that population and you try to grow a culture of belonging to that organization.

So I absolutely agree that access should be reduced to the minimum necessary to ensure operations of the facility.

I think of my experience in the port environment. When we looked at the maritime sector right after 9/11, a wide-open environment for obvious reasons. You want stuff to freely move in and out.

The first answers we got back from the maritime sector were, it is impossible to close this down.

But over time we did that. You set a series of standards that have to be met, an expectation that there will be periodic, random and other types of inspections, that you are subject to it, growing a sense of a culture that we are all in this together.

So as I look at the aviation environment, I look at the hundreds of different employers of people who hold badges, and you think, how do I get that group of people to think as one, to recognize that this is their airport?

So there is a campaign out there. I think that a combination of reducing access points, increasing—setting specific standards for what we expect to be going through those access points, how you inspect to those standards, keeping that randomized expectation of inspection because I think that helps. You need a number of these things. Then growing a sense amongst the workforce, the large number and large percentage of which are good, solid, you know, hardworking people that, look, it is their responsibility to help police this as well.

There are some airports out there that have done this and they have done it very effectively. I would like to look and see what those best practices are and extend those across.

I am looking at the Aviation Security Advisory Committee recommendations. As you know, they had very strong opinions about access controls. I will be meeting with that group in the course of the next few weeks. I am meeting with the airport executives, meeting with the Airports Council. This is a top issue of concern to me as well.

Mr. KATKO. Certainly to follow up, there are a couple of airports Nation-wide, namely Miami and Orlando, and I think Atlanta is going towards this, if they are not already there. Atlanta and Miami out of necessity for criminal conduct that was going on there on their properties.

But those three airports, including Atlanta being the largest airport in the world, I believe the busiest airport in the world, are all going towards 100 percent screening of employees.

Now, we hear from airports across the country again and again that is simply not doable. I would like to hear your thoughts on that.

Mr. NEFFENGER. Well, I am going to start with a visit to those airports and I am going to do that over the course of the month of August, because I want to see what 100 percent security looks like. I want to hear from them how they achieved it, what are the challenges and what are the on-going implications, because I need to be able to address that when I visit with the airports who claim that they can't do that.

So I am on a little fact-finding mission over the next month to try to educate myself as to what the various arguments are and what I would like to do is continue to have this conversation going forward and when I—after I do that.

Mr. KATKO. I look forward to it, sir.

Chairman MCCAUL. Okay, thank you.

Mr. KATKO. Thank you.

Chairman MCCAUL. Miss Rice is recognized.

Miss RICE. Thank you, Mr. Chairman.

Mr. Secretary, I would like to just talk first about diversity. Now, I think gender diversity is a goal for most public and private sectors, but I think for TSA, it is actually an absolute necessity, given the traveling public that they are interacting with on a daily basis. What percentage of TSA employees are women?

Mr. NEFFENGER. I don't have that number off the top of my head, although I have asked for that and it is one of the—it is one of the things I am talking about this week. Diversity, as you know, is critically important.

I will say that, just anecdotally speaking, I have been pleased to see what looks to be a very diverse front-line work force as I travel around. I will get you the percentage of women that we have, and I will break it up by categories, too. Overall, TSOs and the like, going up.

I think that diversity is the key to success in an organization. Always has been. It is one of the biggest challenges we faced in the Coast Guard and in the military, was not just recruiting, but retaining a diverse-looking work force, and we found out early on that just recruiting wasn't enough to call yourself diverse, if there is no pathway up through the organization.

So what I can commit to you is that it is of critical importance to me across the organization and not just in the entry level, but throughout the organization and to look for opportunities throughout.

Miss RICE. I am glad to hear that, because I think that there are limitations placed on female employees that male employees do not have, given how, if you—say you were to have a female employee at baggage, but actually needing to be pulled over to passenger pat-down area because of the need to have more women, only being—you know, women only being able to pat down women, and I think that probably leads to some level of the frustration that female employees have because they are facing those kind of limitations, and room for upward mobility that men just don't.

So I am glad that you are focused on that. Well, I am happy to be sitting here with you. I think that you were a great choice. I think that your focus on trying to improve the morale for your employees is a good goal, and I want to offer that we are here to improve your morale, such as it is, because you are in a truly thankless job.

I look forward to seeing you out in Los Angeles when we go look at LAX airport on the 18th of this month, and I can assure you that we all stand ready to help you in any way that we can.

Thank you, Mr. Chairman.

Chairman MCCAUL. Thank you. The Chair recognizes Mr. Carter.

Mr. CARTER. Thank you, Mr. Chairman.

Admiral, welcome. I in no way speak for all Members of this committee, but for myself, and I suspect that the committee Members would agree with this, we wish you success. We want to see you succeed and we want to do everything we can to help you. I want to touch very quickly on just two things.

First of all, understand that I represent the coast of Georgia, the entire coast of Georgia, and on the coast, we have two major ports. We have the Savannah port, which is the No. 2 container port on

the Eastern Seaboard. We also have the Brunswick Port, which is the No. 2 roll-on roll-off port in the Nation.

Both of those ports are vitally important, and in both of those ports, we use the TWIC cards, the Transportation Workers' Identification Credentials, and I want to talk just briefly about that, very quickly. It—I would like to read to you some examples of situations that have occurred with the TWIC cards that I am very concerned about.

First of all, an individual used a TWIC card to gain access to the Norfolk naval station and killed a naval officer. An individual drove through a gate at a Coast Guard station and threatened to detonate a bomb, demonstrating that a terrorist could do the same, and the ineffectiveness of the TWIC program.

TWIC holders have committed crimes in secure port areas, demonstrating TWICs are provided to criminals and can be used to commit crimes on ports. The proposed rule making for TWIC describes multiple possible terrorist scenarios where the TWIC cards will not be effective.

DHS has failed twice to complete successful pilot programs with the TWIC cards. DHS has not completed a reliable analysis of the TWIC program's internal controls or effectiveness, and finally, GAO has demonstrated the TWIC program's weakness through its analysis invert—in covert testing multiple times.

My question is: What about the TWIC cards? Can it be fixed, and if it can, how are you gonna fix it?

Mr. NEFFENGER. Well, I mean, you raise a lot of—exactly the same questions I have coming into this job. As a former member of the Coast Guard, we worked with TSA throughout. We—as, you know, the Coast Guard implemented the TWIC card reader program based upon the rules that were set for the issuance.

In general terms, here is how I think about identity cards like that. One, I want them—first of all, I want them issued to a known population, meaning—I want some biometrics on that person, I want to be able to run those against databases that tell me whether or not I have got a criminal actor, and then I want to make sure that the disqualifying factors are the right disqualifying factors for holding that card.

As you know, there was a great deal of discussion about what those disqualifying factors should be at the time that the TWIC was created, and a lot of groups, longshoremen and others, had some concerns about that list, and that was a—that took a lot of work to get that list negotiated.

I think you need to continually look at that to ensure that you have got the right features, or the right disqualifying factors, identified, and that you are consistent in that application.

The second piece to it is to have it used properly when you are attempting to enter a facility, and by "used properly," I mean, what aspects of that facility does it give you access to, why does it give you access, and how known are you to the population. So that is part of the reader issue, and it is also part of the procedural and the rules issue.

As you know, there are—the TWIC card can be coded to give you access to different aspects of the facility, some more secure than others.

All of that is my on-going review right now of the program, so while I can't specifically answer all of your questions today, what I promise you is that over the coming weeks and months, I will answer those questions for you, as I get smarter about where we—what the current state of play is.

In your particular instances, I would like more information and detail about what you are saying, because——

Mr. CARTER. Right——

Mr. NEFFENGER [continuing]. I can look at those specifically for you.

Mr. CARTER. Okay, and if I could very quickly, I want to follow up on what Representative Katko had mentioned about vetting on some of the airline workers specifically.

In June we had a hearing here, and I was appalled to find out that some of the applicants for TSA positions were only required to have their last name and first initial and no Social Security number. I hope that that has been taken care of already since that hearing, and if it hasn't, I hope that the first thing you do when you get back is to take care of that.

Mr. NEFFENGER. That has—for those specific ones, that actually absolutely has been taken care of, and we are moving to, as I said, a full name, Social Security number, and clear, you know, clear connection to identity, now.

Mr. CARTER. Good. Well, let me finish by repeating what I said before. We wish you success, and we want to help you. So, thank you, thank you for what you are doing.

Mr. Chairman, I yield back.

Chairman MCCAUL. Thank you. The Chair recognizes Mrs. Torres.

Mrs. TORRES. Thank you, Mr. Chairman, and thank you again, Admiral, for being here with us today. I have no doubt that under your leadership and with your experience, and what it sounds like great support from this committee, you will be successful at addressing the major concerns that we have seen with the TSA, and their responsibility of securing our Nation and our ports.

Today I want to focus on my home airport, Ontario International Airport. As you may know, the airport is controlled by LAWA, the Los Angeles airport. They have oversight and management control of this airport.

Through my experience not only as a passenger but going on a security visit tour of the airport, I want to highlight for you today, the concerns that I have.

Under the agreement, or the arrangement that LAWA has with Ontario, they are—LAX is 56 miles away, and they are the ones controlling our airport. Ontario Airport's manager is only at the airport on a part-time basis. It is a shared position with the Van Nuys airport, which is another, you know, hour away, depending on traffic.

LAWA—we used to have a full-time assistant manager, but that position was deleted a year ago. The authority—the management authority could be very well undermined when that manager is not at Ontario Airport, and it is unclear who is in charge of the airport when that person is physically not present.

When it comes to technology, the Ontario International Airport seems to be lacking. The card reader technology that regulates access to the secure areas is inaccurate, meaning that employees have no limited accesses to where they can enter secure areas. Additionally, many dispatch center security monitors at Ontario Airport are non-functioning.

Ontario Airport gets old fire department equipment from LAX, so whatever is deemed inoperable or unwanted at LAX is shipped to Ontario Airport, and that is the equipment that our folks have to work with.

When it comes to security, the airport's perimeter, security appears to be lacking and needs to be reviewed.

For example, as a result of a grade separation on the north side of the airport, we have had residents able—that were able to walk and drive all the way through to the runway without being stopped.

I also have concerns about the training of Ontario Airport employees. It appears that the LAX employees do some training at the Ontario facility, but it is not clear if our employees at Ontario Airport are participating in that training. As you can see, I have many concerns about the security of Ontario International Airport.

This is a major problem, because the airport serves millions of residents in California, in the Inland Empire. It is a hub. It is an engine for our community in the Inland Empire.

My goal here, as I explained to you earlier, is not to pit or get into the politics of who owns the airport. My goal here today is to ensure that you fully understand the issues and concerns that our community has as it relates to security and who is managing and who is responsible for the Ontario Airport.

At this time, I want to invite you to participate in a meeting with me to discuss these concerns and to come up with solutions to these problems. Would you be willing to discuss these issues and visit with me at the airport and also will you be willing to work with me and other relevant Federal officials to begin to address the tremendous problems that I have seen—personally witnessed at this airport?

Mr. NEFFENGER. Yes, I would be and I look forward to the opportunity to talk to you in more depth to understand better what the issues are and, more importantly, to visit the airport and see for myself what the—what some of these issues are.

Mrs. TORRES. Thank you. I also want to just reiterate that I do get the Ontario Airport experience once a week when I go home. Yield back.

Chairman MCCAUL. Mr. Ratcliffe.

Mr. RATCLIFFE. Thank you, Mr. Chairman.

Admiral, first of all, I would like to thank you for your 34 years of dedicated service in the Coast Guard, and I certainly wish you the best of luck in your new role as the TSA administrator. You have got a very difficult job ahead of you.

As a number of our recent hearings in this committee have highlighted, there are some immediate and frankly glaring problems that you will need to address in this new role.

We need to only rewind the clock a few days to underscore some of the troubling gaps that exist right now at TSA. I am sure that

you are obviously aware that 3 days ago, on Sunday, at the Dallas-Fort Worth Airport a 26-year-old man was able to bypass TSA Security without a boarding pass or any identification at all and get on a plane to Guatemala. According to the police report, it was only after the police were called and the individual left the plane that TSA's security became aware of the incident.

So I want to give you an opportunity to respond to what happened at DFW and give us any information that you can about your investigation into how a breach of that magnitude was possible.

Mr. NEFFENGER. Well, I share your great outrage over that. As I said before, the checkpoint is a very critically important element of a security system and it does form the barrier between. So, with that specific case that is under investigation right now, I am happy to share the results of that with the committee once we see what the specifics were that caused that.

But the bottom line is is that you should not have—it should not be easy, it should be impossible for somebody to make their way past a checkpoint without being observed and certainly should not be possible to get past a checkpoint to the point of getting on an aircraft without having known about it.

So we will find out what happened there. But it speaks, as I said earlier, to the more systemic question about how we are managing our checkpoints. I think it ties right into some of the concerns with respect to how we are supporting our front-line workforce, what the training is, and what the standards are that we expect and, as I said, I think we will find out what happened there, and I will make sure that we put into place the procedures to keep it from happening again.

It may be question of changing the way those barriers are constructed when there is nobody manning a station. It is quite often a case that you have in slower periods lines that aren't open. I want to know how those are secured during that time and what is the protocol for keeping those secure.

Mr. RATCLIFFE. DFW is an airport that I use frequently and, obviously, many of the constituents that I represent as well. It is obviously one of the busiest airports in the country. Can you at least tell us at this point, do you know—is this an issue that was specific to the DFW airport or are some of the concerns here something that could happen at other airports around the country?

In other words, do you know if this is simply a configuration issue or is it a breach of protocol or procedures? Can you share any information at this point in time?

Mr. NEFFENGER. As I said, we are—because it just happened, I haven't seen the report of the investigation; the Office of Investigations is looking at that right now. I will let you know what specifically was the issue here. My suspicion is, is that right now it is confined to that specific location in Dallas-Fort Worth, but I have ordered a full review across the system—I talked to our head of operations at TSA headquarters and said, look, I want you to look across the whole system and tell me whether we have got issues like this elsewhere. If we do, I want to plan for how we are going to address those.

Mr. RATCLIFFE. Admiral, obviously, that unfortunate event at DFW highlights the challenges that you face. I certainly do wish you luck and I look forward to having you work with this committee to improve airport and airline safety in this country. Thanks for being with us today.

I yield back.

Chairman MCCAUL. Let me just comment. I thank the gentleman for raising this issue. Myself, being from Texas, would like a report from the TSA on this incident. It is very disturbing. I don't know how he got past security completely untouched and we don't know anything about this individual either, I assume at this point in time.

Mr. NEFFENGER. What I can tell you is that the reports are that he was distraught over his girlfriend heading out of town and he wanted to stop her, and that is what I know. So it looked like a love-gone-wrong at this point. But we will see, and I am—certainly, I will share with this committee the—our findings on this.

Chairman MCCAUL. Okay, thank you so much.

Mr. Keating is recognized.

Mr. KEATING. Thank you, Mr. Chairman.

Congratulations, Admiral. Thank you for your service with the Coast Guard and thank you for your comments here today. Certainly stressing accountability and doing the kind of work you did in review. It is a difficult assignment but I think you are right on target.

I just want to concentrate on one area which has been something I have brought up for the last several years that represents, I think, a tremendous security issue regarding our airports and that is the perimeter security issue.

Dating back from the time I was a district attorney in Massachusetts, there was a case of a 15-year-old—young 15-year-old boy stowing away on a commercial airline from Charlotte Douglas and tragically losing his life over Milton, Massachusetts, when the landing gear went down. The fact that he penetrated that security aroused the concern.

But we have followed that issue forward and just to put it in perspective, from 2001 to 2011, there were 1,388 perimeter security breaches in our 450 domestic airports. What is troubling, among other things, is that the joint vulnerability assessments as the risks seem to be getting greater, are going down.

Just to give you an idea, from 2004 to 2008, there were 60 of those assessments for our 450 airports. From 2011 to 2013, that was reduced to 30 assessments annually. In 2014, only 12 of those assessments were covered.

That is—that means 97 percent of our Nation's airports weren't reviewed for security risk despite the fact that we have had time and time again whether it is in Chicago or Philadelphia or Los Angeles or, again, in Charlotte Douglas, in New York, we have had these kind of breaches that have occurred. Scores of them have been people that have reached access to the runway and the airports and their refueling areas as well. If a 15- or 16-year-old can penetrate our security—in one instance not even go detected after they reviewed it—then we are vulnerable.

If they can do that and stow away themselves, someone with a different motivation could stow away an explosive on those airlines and not even risk their lives doing it.

I hesitate to keep saying this publicly because I don't want to give people ideas but nothing has been done in terms of progress.

That is why when I wrote you congratulating you on your assignment—I was very pleased to get a response—a timely response back just this month, I appreciate that—where you are identifying this as a priority.

I just want to ask you where you are going with that because it is important and I also—the Chairman and I, when we were working together in Homeland, we had a field hearing and one thing that was so obvious to us was the fact that there is a huge jurisdictional issue at these airports. If things go wrong, they end up pointing the fingers at each other.

They are run by municipal airport organizations, they are run by authorities, and this jurisdiction battle unresolved, even when the Federal Government comes in and said with these assessments, you have things you have to clean up. You have dangers that are here. They don't do it and no one seems to make them do it.

So when you are doing that review, the other thing I think we have to clear up is this jurisdictional issue and if people are going to be safe, they are going from one airport to another. They are in the network. So you are only as good as your weakest link. We are not even assessing more than 3 percent of those airports for safety.

So I want to just give you a minute that is left just to try and expand upon what you wrote me about going forward and dealing with this issue and to try and deal also with this jurisdictional problem that we have.

Mr. NEFFENGER. Well, Congressman, you raised a number of important issues. Let me start by saying I absolutely agree that perimeter security is a concern and, again, I use my experience from the port environment, you know, that that was one of the biggest challenges we had was trying to understand what—first of all, what is the perimeter and what does secure mean?

The joint vulnerability assessments that you mentioned, as you know, those are additional kind of multi-agency assessments that are done in addition to the annual inspection that is done of a system.

So there is a TSA regulatory requirement that we fulfill by inspecting the regulated area of the airport includes a perimeter on an annual basis, and then the joint vulnerability assessments are designed to see what beyond the perimeter—but beyond our immediate jurisdiction might also pose a risk to the airport.

Those are very important in concert. So I want to make sure that the ratio of those is correct and I will look at that.

I also need to attend one of these inspections to find out what they consist of. So I intend to do that. Anyone on this committee is welcome to join me when I do that and I will make the offer to the committee and to the committee Members because I am very interested in how we are doing that.

Again, this is—it goes back to my days trying to figure out how to secure port environments. We—it is the same thing we did. I said, well, just walk me around and show me what a perimeter

looks like. What does that mean? You know, how do you secure that space? How do you secure that space?

The jurisdictional issue is key because you are right, there is a—you can do the Scarecrow in "The Wizard of Oz" thing and just point at everybody but yourself when the jurisdiction comes.

So I need to clearly understand, first of all, what are the extent of my authorities to direct action, and then what are my extent to compel that action if I think it needs to be done?

Ideally, you do that in a partnership, and you do that because it is in everyone's best interest to make sure. From my perspective, I think the airports, the airport count, the airlines and others, would find it of great benefit to ensure that nobody gets on that field that shouldn't be on that field.

Mr. KEATING. Well, thank you, Admiral.

I must tell you, I am optimistic, given your background in the Coast Guard, understanding perimeter issues the way you do, that we are going to meet with some success. I look forward to working with you. If you could report to myself and the committee what your progress will be on this, we deeply appreciate it. Thank you. I yield back.

Chairman MCCAUL. Mrs. Watson Coleman.

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

Congratulations to you, Admiral. You are very encouraging, and it seems that you have taken this assignment on with all high expectations, and with respect to those that get the job done, on behalf of all of us. So thank you.

I just have a couple of little questions. No. 1 has to do with the Federal Air Marshal Service. My understanding is that there hasn't been a class, a recruitment, for nearly 4 years. So I am wondering, do you have any plan to address the attrition that this might represent? Are they still as necessary? Or is there something that is replacing the need for them?

Mr. NEFFENGER. Well, thank you for that question. As you know, we have a new director of the Federal Air Marshal Service, Director Rod Allison. I am really encouraged and enthusiastic about his approach, because he has come in with a very innovative and fresh set of eyes to look across the range of missions of the Federal Air Marshals.

I believe that there is still value in having the Federal Air Marshal Service. I believe that they perform valuable missions. But I believe that those missions have changed over time. Director Allison is addressing some of those changes.

As you know, they work a wide variety of missions, not just the aviation mission that most people are familiar with. But they also work on our VIPR teams, they serve in Joint Terrorism Task Forces, and they bring a unique credentialed law enforcement perspective to—in thinking about the transportation role to those worlds.

That said, we have not hired for a long time in the Federal Air Marshals. We have a request in our fiscal year 2016 budget to begin hiring process. That is an aging workforce. Fifty-seven is mandatory retirement. Over the course of the next 5 years, we will see some—I think the number is—I will get it exact for you, but we will see some 30 percent of that workforce begin to age out.

You need to—when you have a law enforcement agency, a Federal agency, you need to refresh it. We need to grow new people into it. So I am hoping that our fiscal year 2016 budget request will be met favorably. I hope that we can begin to hire into the attrition that we are seeing; and more importantly, grow a new workforce into that as that mission changes over time.

Mrs. WATSON COLEMAN. Thank you. Another area that struck me, as I was preparing for today, has to do with the Secure Identification Display Area cards, the credentials. I understand that on occasion, individuals who have had access to those cards have done things which were illegal, and which just were not acceptable.

So I was wondering, what is the—what are your plans with regard to greater accountability of those cards?

Mr. NEFFENGER. Well, I think accountability is the key. As we were discussing earlier, you have a known—what should be a known and trusted population that you give those cards to. They do get vetted for criminal background history, and they get looked at continuously for potential nexus to terrorism.

That said, we also know that even in known and trusted populations, you can have criminal activity that occurs. We have seen enough evidence of that over the past year.

So one of the things that came out of the incidents that were—or the arrests at Atlanta last year for the drug-smuggling ring that was discovered, was the request by the secretary of the Aviation Security Advisory Committee to take a hard look at the insider threat problem and the use of badges. They came out with 28 recommendations as a result of that.

We have accepted all 28 of those recommendations, and we are working very closely to implement those over time. A number of those were done immediately. Accountability was one of the ones that was done immediately.

I am very concerned about accountability for—it doesn't surprise me that people can periodically lose their badges or misplace them, but there needs to be a process for an immediate notification, for an immediate shutting down of that badge, and then take whatever action is necessary in the event it was done in a deliberate or intentional manner.

Mrs. WATSON COLEMAN. Thank you, Admiral. You have a big task ahead of you. I wish you the best of luck, and I hope that we can be helpful to you in what you need on our behalf. Thank you.

Thank you, Mr. Chairman.

Chairman MCCAUL. Thank you. Let me close by saying I think the Secretary chose the right man for the job. We have enjoyed our conversations over the past several days. I look forward to working with you to improve both the safety of our airports, and also making it more passenger-friendly.

The committee Members may have additional questions in writing. Pursuant to the committee rules, the record will be held open for 10 days. Without objection, the committee stands adjourned.

[Whereupon, at 11:30 a.m., the committee was adjourned.]

APPENDIX

QUESTIONS FROM HON. SCOTT PERRY FOR PETER V. NEFFENGER

Question 1a. Public service is a public trust and many Americans are concerned about pervasive misconduct by TSA personnel. Congressional watchdogs have raised alarms about TSA's lack of focus on misconduct. Specifically, a 2013 GAO report entitled, *TSA Could Strengthen Monitoring of Allegations of Employee Misconduct* states "TSA does not have a process to review misconduct cases; therefore it is unable to verify whether TSA staff is complying with policies and procedures for adjudicating employee misconduct."

Last week, my subcommittee staff requested data from fiscal year 2013–2015 on the number of TSA investigated and adjudicated misconduct cases. TSA told my staff they would have to do data calls to all airports for the information.

Do you find it troubling that TSA does not maintain data on employee misconduct?

Answer. The Transportation Security Administration (TSA) maintains data on employee misconduct and is committed to the highest standards of public trust. TSA actively retains employee misconduct data within a centralized case management system, or Integrated Database, commonly known as the Employee Relations Case Management (ER CM) System. The data requested from fiscal year 2013–2015 on the number of TSA investigated and adjudicated misconduct cases was provided to subcommittee staff on July 29, 2015.

The Government Accountability Office (GAO) requested and analyzed data associated with fiscal years 2010 and 2012 and retrieved from the TSA ER CM, in its 2013 Report 13–624 entitled, *TSA Could Strengthen Monitoring of Allegations of Employee Misconduct.* Following its analysis of TSA misconduct data, the GAO report indicated that "47 percent of the cases that GAO analyzed resulted in letters of reprimand, which describe unacceptable conduct that is the basis for a disciplinary action; 31 percent resulted in suspensions of a definite duration; and 17 percent resulted in the employee's removal from TSA. The remaining cases covered a variety of outcomes, including indefinite suspensions."

Question 1b. Why doesn't TSA have an ability to track misconduct, considering how pervasive misconduct has been?

Answer. TSA has the ability to track misconduct and uses its centralized case management system, ER CM, to continuously monitor and track allegations of misconduct.

Question 1c. What are your plans to fix this problem?

Answer. TSA will continue to capture and track employee misconduct information using its current ER CM centralized case management system. Additionally, TSA has increased management oversight of the investigative and adjudicative processes, and is taking action to develop and implement procedures in four areas to strengthen monitoring misconduct cases, as highlighted by the GAO Report. Specifically, the 2013 GAO Report provided four recommendations for improving TSA's management and oversight of efforts to address allegations of employee misconduct:

1. TSA should establish a process to conduct reviews of misconduct cases to verify that TSA staffs at airports are complying with policies and procedures for adjudicating employee misconduct.

To address this recommendation, TSA currently utilizes a Management Control Objective Process to periodically audit misconduct cases. The audit is designed to mitigate risk and ensure that TSA staff responsible for adjudicating misconduct issues are compliant with internal TSA policy and procedure. These audits are conducted by the Office of Human Capital, Employee Relation Branch, at a minimum, twice annually.

2. TSA should develop and issue guidance to the field clarifying the need for TSA officials at airports to record all misconduct case outcomes in the Integrated Database (ER CM).

TSA has revised its case management guidance for field users to require that all corrective, disciplinary, and adverse actions must be recorded into the ER CM for all employees. Additionally, customized training is provided to field users to further educate on the ER CM process.

3. TSA should establish an agency-wide policy to track cycle times in the investigations and adjudications process.

TSA developed agency-wide policies, which identify process areas needing improvement, and developed new data fields that have been incorporated into the Integrated Database to track cycle times.

4. TSA should develop reconciliation procedures to identify allegations of employee misconduct not previously addressed through adjudication.

TSA Employee Relations, in the Office of Human Capital, is responsible for overseeing and reviewing disciplinary actions handled by TSA management at airports, as well as managing the ER CM. TSA is developing guidance that will capture final outcomes within the ER CM for cases which are: (1) Opened for investigation, (2) adjudicated with a penalty outcome, or (3) adjudicated with no penalty outcome. This change in the TSA internal process will strengthen managerial oversight, assist with reconciling process gaps, and ensure that TSA maintains complete institutional records associated with the investigative and adjudication processes.

Question 1d. With TSA employee misconduct an on-going and egregious issue, what are you doing to ensure that misconduct cases are taken seriously and handled accordingly?

Answer. In addition to the above, TSA continues to provide training tools that will better prepare agency managers and supervisors to accomplish TSA's security mission, manage employees effectively, and understand the agency's expectations related to conduct and performance. For example, TSA has developed and implemented a process to evaluate and analyze cases to ensure that airports comply with policies and procedures for adjudicating employee misconduct. On a monthly basis, TSA evaluates compliance with requirements, identifies areas for improvement, discusses trends and best practices with airports as appropriate, and briefs Senior Leadership on these trends to ensure continued compliance with policies and procedures.

Question 2a. The Federal Air Marshal Service is the primary law enforcement entity of the TSA—deploying air marshals on domestic and international flights to detect, deter, and defeat hostile acts targeting U.S. air carriers, airports, passengers, and crews. According to TSA, "successful accomplishment of the Federal Air Marshal's mission is critical to civil aviation and homeland security." However, a 2015 news report highlighted an investigation into a FAMS flight coordinator who manipulated the system and "used her position to look up personnel files, identification photographs and flight schedules to pinpoint air marshals she was interested in meeting and possibly dating."[1][sic] This is just one recent example. Reports of misconduct within FAMs are nothing new; in 2012, the Inspector General also examined misconduct allegations in FAMS and made 12 recommendations for TSA.

How have TSA personnel that were involved in this misconduct been held accountable?

Answer. This matter is under investigation with the potential for criminal prosecution. At the close of the investigation, the appropriate action will be administered by the Transportation Security Administration (TSA) for any employee identified in the investigation to have committed a violation of law, regulation and/or policy, up to and including removal, or forwarding for prosecution.

The TSA holds all of its employees to the highest standard of professional and ethical conduct. Accusations of misconduct are investigated thoroughly and, if substantiated, appropriate action is taken. The vast majority of TSA personnel are hardworking individuals who perform with integrity each and every day. As an agency, TSA strives to instill a culture of accountability throughout the workforce. While TSA will not comment publicly on internal disciplinary actions, the agency has zero tolerance for misconduct or discrimination in the workplace.

Question 2b. What safeguards are in place to make sure an occurrence like this is not possible in the future?

Answer. TSA employees are required to complete annual *Employee Responsibilities and Code of Conduct* training in accordance with TSA Management Directive (MD) 1100.73–5. This policy requires employees to report "any known or suspected violation of law, rule, regulation, policy, or Standard Operating Procedure by a person to any manager in the chain of supervision and/or to the Office of Inspection (OOI)." Furthermore, Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) personnel are required to annually certify and acknowledge the OLE/FAMS

1112 *Employee Responsibilities and Conduct* policy at the beginning of the employee's performance review.

In addition, TSA established a new Assessments and Evaluation Unit (AEU) in December 2014, whose primary focus is to monitor and ensure quality assurance checks are conducted in all facets of the FAMS Systems Operation Control Section (SOCS). To achieve the highest standard of controls, AEU has placed concentrated efforts on the following mitigation efforts:

- Implementation of a quality control call system to observe employees for compliance with their Standard Operating Procedures;
- Addition of extensive audit reports to the Airline Reservations System to identify possible fraudulent activity;
- Methodical training of the SOCS Management team on analytical techniques to identify possible fraudulent activity made within the FAMS scheduling system.
- Review of all Standard Operating Procedures within the SOCS; and
- Implementation of restrictive controls on all system accesses with a focus on the Airline Reservations System to the FAMS Scheduling Application.

To date, AEU has reviewed over 13,000 aircrews schedule changes and over 1,100 reservation changes with no identified fraudulent activities. Over 3,300 access control profiles on the Airline Reservations System were reviewed and the required accesses verified.

QUESTIONS FROM RANKING MEMBER BENNIE G. THOMPSON FOR PETER V. NEFFENGER

Question 1. Since 2007, we have spent over $700 million on the Behavior Detection Officers program. As you know, the Government Accountability Office noted that this program could not be scientifically validated, and even suggested that Congress consider limiting funding for the program. What are the plans for Behavioral Detection Officers going forward?

Answer. The Behavior Detection and Analysis (BDA) Program is an integral part of the Transportation Security Administration's (TSA's) security program; providing real-time threat assessments based on behavior pattern recognition techniques that detect behavior indicators and suspicious activities that deviate from an established environmental baseline.

TSA strongly disagrees with the Government Accountability Office (GAO) assertion that the program is ineffective, and non-concurred with the recommendation to limit funding. In 2007, in an effort to validate TSA's behavior observation techniques, the Department of Homeland Security engaged the American Institutes for Research to examine the validity of the program in the context of checkpoint screening. The study's findings revealed that TSA's program is 9 times more effective than random selection at identifying high-risk passengers. In 2012, TSA initiated further review of its Behavior Detection program contracting with an independent third party to determine the optimal categorization of indicators. The substantiated and revised set of behavior indicators use the most current behavior detection research from the scientific community.

There are many examples of behavior detection strengthening TSA's security posture. The following cases illustrate the vital layer of security that Behavior Detection Officers (BDOs) provide:

- In Buffalo (BUF), in 2009, Behavior Detection Officers (BDOs) referred a passenger and his traveling companion for additional screening, and discovered $9,500 in U.S. currency, and that the passengers were traveling from BUF to New York (JFK) en route to Yemen. In July 2015, one of these passengers was charged with attempting to provide material support to ISIL. While the BDO referral did not lead directly to arrest, the additional screening received based on referral ensures the passenger was not traveling with dangerous items on that trip.
- In New York (JFK), BDOs referred a passenger for additional screening due to suspicious behaviors, and discovered suspected fraudulent DEC and NYPD badges, and a police jacket in the passenger's carry-on bag. Port Authority Police responded and interviewed the passenger, who stated he was going to Haiti on police business. Law Enforcement Officers (LEOs) confiscated the badges and arrested the passenger on a state charge of impersonating an officer. Also at JFK, BDOs engaged a passenger who turned out to be an insider who was attempting to circumvent security. BDOs determined that the passenger had a carry-on bag that was transported through the Known Crew Member entrance by a flight attendant. LEOs located the flight attendant, who was rescreened with the accessible property and denied boarding. On 10/3/2015, at JFK, BDOs engaged an individual in a security-related question that exposed an attempt

to circumvent the screening process by an airline employee. Based on the interaction, BDOs were able to determine that the passenger had a carry-on bag that was provided to a flight attendant, whom attempted to transit through the Known Crew Member entrance circumventing screening. LEOs were notified, identified the flight attendant whom was rescreened, and denied boarding.

- In Orlando (MCO), BDOs observed a passenger behaving suspiciously during the check-in process. When the passenger presented his checked baggage to the airline, the BDOs referred the bags for secondary screening. During the checked baggage screening, TSOs discovered a battery, wires, an end cap pipe with holes in it, lighter fluid, and literature detailing how to build explosive devices. TSOs also discovered two bottles containing a blue liquid which tested positive for TNT. The FBI charged the individual with attempting to introduce an explosive or incendiary device on an aircraft.

In addition, TSA has realigned Behavior Detection Officers (BDOs) to higher-risk airports, while reducing the full-time BDO footprint from 122 airports to 87 airports using a risk-based staffing model. The fiscal year 2016 President's request includes a 15 percent reduction in BDOs from 3,131 to 2,660 to align to this staffing model. It is important to note that approximately 97 percent of the Behavior Detection and Analysis Program's budget goes toward officer personnel costs and benefits. To offset this reduction, TSA created a spectrum of capabilities where a certain number of existing TSOs receive behavior detection training and certification. The certified TSOs conduct traditional screening 80 percent of the time per pay period, and 20 percent of the time conduct behavior detection-related functions to support TSA's risk-based security initiatives. The multi-function capability provides lower-risk airports with behavior detection mitigation tools where otherwise the risk model would not have dedicated a full-time behavior detection capability.

Question 2. Administrator Neffenger, TSA is most visible and receives the most attention surrounding its efforts to secure commercial aviation from attacks, such as those perpetrated on September 11, 2001. Although the budget for surface activities has grown, it is still relatively small when compared to that used to address commercial aviation activities. With the threats to our Nation constantly evolving, and encompassing other modes of transportation outside of commercial aviation, how do you plan to address threats that possibly target other modes of transportation?

Answer. The Transportation Security Administration (TSA) has a strong focus on commercial aviation where demonstrated risk is the highest, and the Federal role is more prevalent. In the non-aviation sector, TSA has an active and growing partnership role in reducing risk in all surface modes and is dedicated to an intelligence informed risk-based approach to security.

TSA's role in surface is focused primarily on oversight, voluntary compliance, cooperation, and to a lesser extent, regulation. TSA could not accomplish this essential mission without our partners voluntarily adopting security improvements and sharing best practices with each other and with us. This collaborative "whole community" approach ensures that resources are applied efficiently to have the highest efficacy in reducing risk. Collaboration happens both informally on a day-to-day basis, and through formal structures like the Department of Homeland Security (DHS)-led Critical Infrastructure Partnership Advisory Council framework, Sector Coordinating Councils, and other industry-centric organizations, such as the Mass Transit Policing and Security Peer Advisory Group (PAG). Our participation in forums such as the annual Mass Transit and Passenger Rail Security and Emergency Management Roundtable, and our continuing work with the PAG enable us to understand the security needs of our domestic and international security partners, to better tailor our programs and resources to meet critical needs. We also work very closely with our stakeholders in the development and dissemination of recommended practices, such as Security Action Items (SAIs) for mass transit, highway, and freight rail; motor-coach security best practices; and the Pipeline Security Smart Practice Observations.

TSA also plays a role in surface transportation security through voluntary assessments and regulatory compliance inspections. Both mass transit and freight rail providers operate within TSA regulatory oversight. We conduct 10,000 regulatory inspections of freight railroads each year on rail cars carrying Rail Security Sensitive Materials. TSA also conducts voluntary assessments of security programs and plans on the 100 largest mass transit and passenger rail systems (based on passenger volume), which account for over 95 percent [1] of all users of public transportation, through the Baseline Assessment for Security Enhancement (BASE) pro-

[1] American Public Transportation Association Average Daily Ridership Statistics *http://www.apta.com/resources/statistics/Pages/default.aspx.*

gram. The BASE program is a thorough security assessment of mass transit and passenger rail systems nationally. Results of these assessments, as well as similar assessments and analyses in all the surface modes, guide the development of risk reduction plans and initiatives to provide our security partners with a menu of risk mitigation options they can implement based on threat and their specific capabilities.

TSA recognizes those agencies that have performed exceptionally well in their assessment during the fiscal year with a Gold Standard award. The criterion for achieving the Gold Standard in security is to attain high scores across all 17 categories of assessment, with no one category receiving a low score that may indicate a potential vulnerability.

As part of its surface transportation security responsibilities, TSA manages vetting programs for specific surface modes. Specifically, TSA's Hazmat Endorsement Program has vetted over 2.8 million commercial drivers of hazardous materials since its inception in January of 2005. Similarly, TSA's Transportation Workers Identification Credential Program has vetted over 3.3 million transportation workers seeking access to secured maritime facilities since its inception in October of 2007.

TSA's partnership with stakeholders extends to voluntary security guidance, exercises, and training programs implemented in surface modes. TSA has conducted thousands of security assessments, provided security enhancement guidance, and conducted security training and exercises. Through close work with our partners, we develop resources for security training and exercises, such as TSA-produced training modules and the DHS-sponsored "Run, Hide, Fight" Active-Shooter training. We also have the TSA First Observer™ program, which trains highway professionals to observe, assess, and report potential security and terrorism incidents. We also feel that practice through exercises is exceedingly important. As such, we collaborate with industry through our Intermodal Security Training and Exercise Program (I–STEP) to help surface entities test and evaluate their security plans and ability to respond to threats with other first responders.

TSA also continues to work with the intelligence community, and shares relevant information in a timely manner with public and private stakeholders to enhance preparedness and vigilance. TSA has also coordinated the distribution of security-bolstering grant funds to hundreds of entities when available, and provides operational security assistance to industry security partners in the form of explosive detection canines, screening support, and Visible Intermodal Prevention and Response teams.

TSA has a strong partnership with the DHS Science and Technology (S&T) Directorate. S&T has a dedicated program focused on countering the explosive threat in the mass transit system.

Question 3. Administrator Neffenger, are there plans to evaluate other technologies outside of those already in use at checkpoints throughout our Nation's airports?

Answer. The Transportation Security Administration (TSA) continues to work with the Department of Homeland Security's Science and Technology Directorate (DHS S&T) and international partners to understand what existing and emerging technologies are available. TSA routinely posts Requests for Information (RFIs) and targeted Broad Agency Announcements on the Federal Business Opportunities website *(www.fbo.gov).* Through these requests, TSA is able to solicit industry for input on the technological landscape.TSA is also working with DHS S&T to further the "Screening at Speed" initiative, which aims to develop the next generation of screening technology.

In addition, TSA recently released its Strategic Five-Year Technology Investment Plan, which aims to achieve a shared vision among Congressional, industry, Department of Homeland Security (DHS), and TSA stakeholders to address security technology needs, deploy cutting-edge security capabilities, and increase efficiency and security effectiveness in American aviation security. The plan builds on the May 2014 TSA Strategic Capability Investment Plan, which was the product of engagement with industry and was published in the interest of helping stakeholders understand the Agency's direction to align investments and product development initiatives accordingly.

The plan provides a cohesive approach for the development and successful transition of security technology solutions, and it lays the foundation for future innovation and meets the immediate technology demands of specific mission needs. TSA and the DHS S&T define research and development goals and objectives to closely align investments with TSA mission needs in efforts to drive tangible solutions and innovations in transportation security.

The plan is an important step to foster mutually-beneficial dialogue and collaboration with industry, academic, and Federal Government partners.

Question 4. Administrator Neffenger, within the past year, there have been recurring reports of incidents in which nefarious characters are using their secure identification display area (SIDA) credentials to bypass screening, and board commercial aircraft with weapons, or what they believed to be illegal substances. Given these instances, and the fact that the airport is responsible for these badges, is there any plan to give greater accountability to the credentialing process by possibly having a universal SIDA badge issuance, status, and recovery process for which the TSA would have responsibility?

Answer. Each Federally-regulated airport is accountable under Title 49 Code of Federal Regulations Part 1542 to have an access control program to limit access to certain parts of the airport to those individuals who require access to do their jobs. These airport access control programs vary with the unique requirements of each airport (e.g., infrastructure, geography, size, proximity to urban areas, etc.). Notwithstanding the otherwise unique requirements of each airport, they must meet the Transportation Security Administration's (TSA) standards for vetting individuals, which are the same Nation-wide.

Based upon statutory and regulatory requirements, vetting performed by TSA includes an intelligence-related check of Governmental databases, including recurrent vetting against the Terrorist Watch List; immigration status check; and a fingerprint-based criminal history records check based on information from the FBI. Airport and aircraft operators are responsible for adjudicating the results of the criminal history records check against the list of 28 disqualifying crimes contained in 49 CFR 1542.209, determining the applicant has a legal right to work in the United States, and issuing the badge. Additionally, Security Directive 1542–04–08J requires airports to resubmit fingerprints for a new criminal history records check every 2 years, or upon badge renewal by the airport, whichever comes first, and to adjudicate the results to ensure no disqualifying crimes have been committed.

Following the discovery and publicized arrests by law enforcement of a weapon smuggling ring at Hartsfield-Jackson Atlanta International Airport in December 2014, TSA requested the Aviation Security Advisory Committee (ASAC) to examine options to address the vulnerability highlighted by the criminal activity. On April 8, 2015, the ASAC submitted its final report with 28 recommendations to improve the control of employee access to restricted areas in our Nation's airports.

With regards to SIDA badge inventory, the ASAC did specifically recommend that TSA create and maintain a National database of employees who have had their SIDA badges revoked for cause. The security benefit of a "revoked badge" database would be awareness of individuals, who were removed for cause from access to one airport would be identifiable to another airport if they sought further airport employment elsewhere. While that capability does not currently exist, TSA is evaluating the feasibility of such a TSA-managed National database, which may strengthen the credentialing process Nation-wide. TSA will establish an Agency-stakeholder working group to explore options for providing a National database. TSA began this process in June. Still, there are significant issues involved, ranging from technological aspects to privacy and civil liberties, which must be fully addressed. Areas of review will cover policy, operational processes, technical modifications, and possible clearinghouses to support the effort.

While TSA examines the possibility of creating a National database, the agency will continue to exercise its oversight of compliance with the regulatory requirements. Each Federally-regulated airport remains strictly accountable to TSA under Title 49 Code of Federal Regulations Part 1542 to have an access control program to limit access to certain parts of the airport to those individuals who require access to do their jobs. TSA inspects to ensure strict compliance by individual airport operators with badge issuance, accountability, and deactivation requirements.

Question 5. Part-time TSOs have reported to their union an increase in mandatory overtime at some airports to address operational needs. As I understand it, TSA can currently increase a part-time TSO's hours up to 32 hours per week for 13 consecutive pay periods. It is difficult to square annual staff reductions with recurring mandatory overtime for part-time TSOs. Why not hire additional full-time TSOs to provide the coverage needed at these airports?

If it is a question of adequate appropriations, do you intend to request additional funds?

Answer. The Transportation Security Administration (TSA) depends on part-time employees to efficiently meet day-to-day surges in passenger traffic. Over the last 2 years, TSA has shifted to a higher percentage of full-time employees through improved management of workforce training and scheduling. Based on the current staffing model, there is a need for a part-time workforce to complement the full-time

workforce and provide the ability to flex staffing levels during high-volume hours. TSA continues to monitor and evaluate its staffing requirements and their corresponding costs.

Question 6. TSA has announced savings from reductions in 1,441 TSO positions based on efficiencies from risk-based screenings. Knowing that you are only a few weeks into this position, I would be interested in the number of management and administrative positions being eliminated by risk-based screening?

Answer. As the Transportation Security Administration (TSA) implemented risk-based security initiatives, operational positions were reduced, and TSA also took commensurate and proportional reductions in managerial and administrative staff. The reduction of 1,441 employees consisted of 1,368 Transportation Security Officers and 73 management and administrative positions in fiscal year 2015. In an effort to support this reduction, TSA completed a thorough review of field staffing requirements at each hub and spoke airport. Following the review, 120 hubs were reduced to 77 hubs, which resulted in a consolidation of resources and reductions in the number of Federal Security Director (FSD) staff as well as administrative staff. Additionally, TSA has an FSD Staffing Model which is based on 11 inputs used to determine the complexity (such as hours of operation, number of terminals, and number of checkpoints) in combination with the staffing headcounts to identify administrative staffing requirements.

Our recent analysis of the covert testing root causes has led us to reassess the reductions projected for fiscal year 2016. As we rebalance our operational focus on increased effectiveness, it will be important to sustain our force size at or above fiscal year 2015 levels in order to avoid jeopardizing our ability to improve checkpoint screening operations.

Question 7. It is essential that TSOs receive active-shooter training that reflects a unique attack at an airport checkpoint, as opposed to an attack on an office building. Disturbingly, TSOs at some airports report that they have had no active-duty training other than a video reflecting an attack on an office building and have not participated in multi-disciplinary drills at the airport. It has been nearly 2 years since the attack on LAX that cost TSO Hernandez's life. Given your limited time on the job, can you give us an update regarding active shooter training?

Answer. Since the tragic event at Los Angeles International Airport (LAX) on November 1, 2013, the Transportation Security Administration (TSA) has implemented multiple active-shooter training events, which all TSA employees have completed. In addition, immediately following the event, TSA mandated that all TSA employees review readily available active-shooter training videos by March 31, 2014. The videos were from the Federal Emergency Management Agency and the Houston Police Department; both videos reflected an attack in an office environment.

During this time, the TSA Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) and Office of Training and Workforce Engagement (OTWE) developed *Active Threat Recognition & Response Training.* The purpose was to provide the TSA workforce an understanding of their role in recognizing and responding to an active threat incident in each type of location where TSA employees work, to include airport checkpoints, baggage areas, airport air operations areas (AOA), and the office. This was instructor-led training, with the Assistant Federal Security Director-Law Enforcement as the primary instructor, and included table-top exercises/discussions. This training was released in June 2014 and had a completion date of December 31, 2014.

During 2014, TSA also developed a new training product, titled "Active Shooter Incident Response Training," for active-shooter incidents specifically depicting an airport environment. The training was designed to reinforce the widely-accepted active-shooter response reactions of "Run-Hide-Fight," and built upon the materials presented in the previously completed training courses. The interactive training video was filmed in its entirety at the Indianapolis airport with the support and participation of multiple airport tenant organizations to include local airport officials, law enforcement officers, and TSA personnel. The training included information that would help the workforce:

- Recognize how to respond when an active shooter is in their vicinity; and
- Identify how to interact with Law Enforcement Officers who are responding to an incident.

In January 2015, TSA released the training video with a required completion date of March 31, 2015; to date over 54,000 TSA employees have completed the training, to include 47,500 members of the officer workforce. TSA has mandated that this be an annual training requirement for its workforce. During the March 2015 incident at Louis Armstrong New Orleans International Airport (MSY), one of TSA's Supervisory TSOs was attacked by an assailant wielding a machete, and was grazed by a bullet as a Jefferson Parrish Sheriff's Deputy fired shots during the attack. Addi-

tionally, the assailant sprayed wasp repellent at three other TSA Officers, minimizing their capacity to react. It was during post-incident discussions with TSA's team at MSY that TSA learned that the team specifically attributed their survival to the "Active Shooter" training that they had received.

Additionally, TSA has distributed over 500 copies of the "Active Shooter Incident Response Training" to airport directors, comprising both private-sector and local public-sector entities, and encouraged them to provide the airport-specific training to airport and airline employees. TSA has also shared the training video with several other Government agencies, as well as representatives of aviation authorities from France and Germany.

TSA has also incorporated an actual "Active Shooter" exercise into its Essentials of Leading Screening Operations (ELSO) course delivered at the TSA Academy at FLETC Glynco, GA. This provides an opportunity for all Lead TSOs, of which TSA has approximately 6,000, to experience a drill that is facilitated at the FLETC Intermodal Transportation Training Building (No. 811) by TSA's Federal Air Marshals (FAMS). The exercise has been praised as a true learning experience for those who have participated, allowing them to experience the sound and impact associated with a would-be attack, followed by a review of what they experienced and discussion of how to prepare themselves for any event similar to the training exercise. While TSA has no immediate plans to replicate this exercise outside of the TSA Academy, it is an exercise that TSA will continue to include in a number of different courses that will be coming to the TSA Academy over the next several years.

Question 8a. In the wake of the Inspector General's covert testing results being leaked, Secretary Johnson appointed a "Tiger Team" of DHS and TSA officials to monitor the implementation of reforms the Secretary announced. It is my understanding from press releases issued by DHS that the "Tiger Team" provides the Secretary with status reports on a rolling 2-week basis.

Did you have any input into who would comprise the Tiger Team?

Answer. The Transportation Security Administration (TSA) Tiger Team was established in early June 2015, which preceded my confirmation and official swearing in on July 4, 2015. Subsequent to my confirmation, I have closely reviewed the composition of the team and the process they are using to assess root causes of the screening failures. I fully support these efforts.

Question 8b. Are you receiving the same status reports from the Tiger Team that the Secretary is receiving?

Answer. Yes, I closely oversee these efforts and personally participate in the updates to the Secretary.

Question 8c. How will the Tiger Team's success or failure be judged?

Answer. We are reassessing our strategic measures of effectiveness and intend to refine our focus on a security proposition that values both effectiveness and efficiency. The success of our efforts to correct the problems identified will be judged by the improved performance and effectiveness of our workforce in detecting and disrupting prohibited items in our checkpoint screening operations. We will continue to use our own covert testing and performance testing to evaluate these improvements, as well as macro assessments of our system effectiveness using a range of analytical tools.

Question 9. Administrator Neffenger, fiscal year after fiscal year, the number of Transportation Security Officers decreases due to the use of risk-based screening initiatives. I am concerned that with such an important mission, the ranks of TSOs could become so thin that the mission is inadvertently hampered. I know that you are about 4 weeks into your current role, but could you speak on this as much as you can, and commit to revisiting this issue with the committee in the future?

Answer. Over the past 5 years, the Transportation Security Administration's (TSA) budget has included multiple efficiencies, with the largest coming from Risk-Based Screening (RBS) savings identified in the fiscal year 2015 and fiscal year 2016 requests, totaling 3,491 Full-Time Equivalents and $239 million. As a result of the findings from the recent Department of Homeland Security's (DHS) Office of Inspector General (OIG) covert testing on TSA checkpoint operations, TSA is aggressively working to determine the proximate root causes of the covert testing failures and provide effective system-wide solutions, which may include adjustments to staffing levels.

Our recent analysis of the covert testing root causes has led us to reassess the reductions projected for fiscal year 2016. As we rebalance our operational focus on increased effectiveness, it will be important to sustain our force size at or above fiscal year 2015 levels in order to avoid jeopardizing our ability to improve checkpoint screening operations.

Looking forward, I can assure the committee that TSA will continually evaluate the staffing requirements and revisit this issue as needed.

Question 10. Administrator Neffenger, last week, the Transportation Security Subcommittee marked up three bills; HR 3102, the Airport Access Control Security Improvement Act of 2015; HR 3144, the Partners for Aviation Security Act; and a Committee Print for a reform and improvement act, which is intended to be a reauthorization. I believe that prudence dictates that we hear your vision and priority for TSA before marking up legislation such as the Committee Print. With that being said, these pieces of legislation need work as they move forward toward full-committee consideration. Will you work with us to address issues with these pieces of legislation, such as those brought about by various labor groups regarding the Access Control Security Act, to ensure that they are as thoughtful and considerate of all stakeholder issues as possible?

Answer. The Transportation Security Administration will be happy to provide technical drafting assistance to Congressional Members, or more formal comments to address issues with these pieces of legislation in our efforts to ensure that they are thoughtful and considerate of all stakeholder concerns and perspectives.

Question 11. During the 113th Session, Representative Julia Brownley introduced the Honoring Our Fallen TSA Heroes Act, a bill that would provide public safety officer death and education benefits to the families of TSOs who are killed or badly disabled in the line of duty. TSOs would join a long line of public servants, including police officers, fire fighters and Emergency Medical Technicians who are eligible for the benefits. Public safety officer benefits serve as a recruitment tool for positions that protect the public, and allow those who answer the call of duty peace of mind that their loved ones will be taken care of if they are killed or disabled in the line of duty. Will TSA support granting TSOs public safety officer death and education benefits under the Honoring Our Fallen TSA Heroes Act?

Answer. The Transportation Security Administration appreciates Congress' efforts to provide individual benefits for the family of Officer Hernandez, and would welcome the opportunity to work with the committee should similar legislation be reintroduced to expand the benefits to all Transportation Security Officers killed or injured in the line of duty.

Question 12a. Administrator Neffenger, a past DHS–OIG report has proven that employee morale is at an all-time low and has been described as "dismal" for TSA. It was also noted that this low employee morale has been possibly impacting the functionality of TSA's operations.

What steps do you plan to take to improve employee morale and employee relations within TSA?

Answer. In my experience, strong and positive morale results directly from a positive leadership approach where leaders care about what matters to those we lead. Successful leaders have an awareness of what compels employees to commit their talents, energy, and effort to any endeavor. In my view, regardless of their generation, what motivates a workforce is for employees to know that their job and their contributions matter, that the work is meaningful, and that each employee can provide value and make a difference. Thus, it will be my intent to ensure that each member of TSA has a clear, well-defined purpose, that the employees know the importance of their mission, that they are trained and empowered to perform their duties, that they are valued and supported in doing that mission, and that leadership provides equitable and consistent accountability, at all levels, as well as appropriate recognition for performance.

Another significant component of morale and performance is the role that leaders play, especially in recognizing the challenges of the day-to-day work, and in responding to those challenges. Leaders must create opportunities to listen, to understand workforce challenges as seen from the employees' perspective. Leaders must also act on the concerns raised, both to advance the mission and to support employees in executing their duties. This can take the form of new training, tools, and procedures or it can be visible through demonstrated support from management in acknowledgement and recognition of the difficulty in executing a no-fail mission.

In addition, TSA is taking several steps to improve employee morale and employee relations within the agency:

- Enhanced Training Support:
  - The Essentials of Leading Screening Operations and Essentials of Supervising Screening Operations training for Lead and Supervisory Transportation Security Officers were launched to improve leadership capabilities on the front line.
  - A new web-based training course is being developed for supervisors and managers that addresses the expectations for employee engagement at TSA, and the specific steps that TSA supervisors in different roles can take to improve their own engagement efforts.

- Increased Communication and Transparency:
  - The TSA Office of Security Operations launched the Operations Network for Employees, which has several phases that are focused on opening communication channels, fostering collaborative and productive working relationships, and introducing employees to new employment opportunities and skill development.
  - More time for airport shift briefings has been added to the staffing model to encourage consistent communication to front-line employees at the start of each shift.
  - Recent changes were made to increase transparency regarding the distribution process for screening workforce performance awards and mitigate the impact of differences in performance ratings across the Nation.
  - TSA is launching an engagement tool kit with resources, information, and best practices for addressing areas of low employee satisfaction such as employee development, recognition, and communication. The release of this tool kit is being timed with the release of 2015 Federal Employee Viewpoint Survey results.
  - TSA created a learning, engagement, and career development iShare portal called Success U to give employees the information and resources necessary to build their skills. Nearly 50,000 unique employees visited the site in its first year of operation.
  - TSA launched a blog called "LEAD!" targeted towards mid- and senior-level leaders to stress the importance of communication, collaboration, and motivation, and to provide examples of good engagement practices.
  - TSA has created a series of Workforce Engagement (WE) initiatives. The acronym WE is a dual-purpose branding mechanism, which seeks to further develop TSA's commitment to workforce engagement, and emphasizes that we are "all in this agency together," and working hard to continuously improve.
- Career Development:
  - The TSA Mentoring Program was implemented to provide interested employees with mentors who can provide career coaching and other support; as of September 2, 2015, over 2,460 employees from 285 program offices have participated.
- The Office of Law Enforcement/Federal Air Marshal Service Career Track Program was developed to provide tools and resources to promote career exploration and self-assessment.
- TSA improved its Leadership Education Program to include eligibility for lower-banded employees, and expanded the course offerings to prestigious universities around the country in order to make the program more accessible, effective, and relevant.
- TSA also improved its Leadership Development Programs to include eligibility for lower-banded employees, partnership with Academic Institutions to provide academic learning and Strengths-Based Leadership Assessments, and reduction in program completion time frames to increase throughput. TSA's Leadership Development Programs have been aligned under the Office of Personnel Management's Executive Core Qualifications and the underpinning competencies to achieve greater standardization across the DHS Leadership Framework and the Federal Government.

Question 12b. Based on surveys and feedback from its employees, has the agency noted any improvements?

Answer. While the Federal Employee Viewpoint Survey ratings related to morale have not indicated significant change in recent years, TSA remains confident that on-going initiatives and efforts under development will yield a positive impact on employee morale in upcoming surveys.

Question 13. On Monday, the Securing Expedited Screening Act passed out of the House and requires that TSA only grant expedited screening to passengers who have been previously vetted, and not through random selection, such as that used in the Managed Inclusion (MI) Program. Please detail for us your thoughts on expedited screening overall, as well as your thoughts on the Managed Inclusion program, because the security effectiveness of MI has been called into question by numerous GAO and OIG reports.

Answer. Expedited screening is a product of the Transportation Security Administration's (TSA) evolution from a one-size-fits-all screening approach to a risk-based security concept. Managed Inclusion (MI), first and foremost, is a process in which TSA applies additional security measures prior to processing through a screening checkpoint by utilizing additional layers of security such as explosives detection (through Passenger Screening Canines or Explosives Trace Detection (ETD)), and observation from Behavior Detection Officers. Up until recently, there were two

types of MI operating procedures. MI–1 employed the use of canines while MI–2 employed the random use of ETD. With the application of these security layers, TSA has the capability to conduct a real-time threat assessment of standard (unknown) passengers. If the standard passenger clears the additional security measures then they would be provided access to expedited screening lanes.

Since the expansion of TSA PreCheck™ and initiation of MI operations in 2013, TSA's methodology has always centered around the reduction of MI utilization in parallel with the increase in TSA PreCheck™ travel population. In line with the methodology established in 2013, TSA is currently reviewing expedited screening concepts with the intent of reducing expedited screening for travelers who have not completed a full biographic and biometric security threat assessment. Therefore, over the course of the past year, TSA has reduced the reliance on MI by approximately 80 percent (high of 16.1 percent over New Year's 2015 to approximately 3 percent today). A major contributor to the reduction of MI utilization was the reduction plan and ultimately the elimination of MI–2 on September 12, 2015. The decision to maintain MI–1 while eliminating MI–2 was mainly in part due to the explosives trace capability, as canines provide a 100 percent screening capability of the passenger queue, whereas the random use of ETD does not.

Question 14. There is currently no permanent solution for military checked baggage originating from Air Mobility Command (AMC) Patriot Express channel mission flights and the committee believes such an effort is a critical layer of security to maintain safety for all passengers who utilize these airports such as with Baltimore/Washington International Thurgood Marshall Airport (BWI) and Seattle-Tacoma International Airport (SeaTac) as their home airport, or as a connection to their final destination. There are no current regulations that require the Transportation Security Administration (TSA) to screen checked baggage from such military flights but it is our understanding that the Department of Defense, namely US TRANSCOM, is in great support of making their aircraft, and subsequently commercial airliners that will receive this baggage, more secure. Can you give us the status of working on a permanent solution for these airports to make sure there is a permanent solution in the near future for the screening of baggage being placed on aircraft?

Answer. The Transportation Security Administration (TSA) has and will continue to coordinate with the U.S. Transportation Command (USTRANSCOM) to ensure the safety of their flight operations. Every airport operation is unique; the favorable solution for screening USTRANSCOM checked luggage is via an airport-owned baggage in-line system. For example, the processing of Seattle-Tacoma International Airport's checked luggage via an in-line system poses a minimal to zero cost for USTRANSCOM. The cost is dependent on existing commercial flight schedules out of the specific baggage in-line system.

At the request of USTRANSCOM, TSA recently provided potential options for a permanent operational process at Baltimore/Washington International Thurgood Marshall Airport (BWI). USTRANSCOM is coordinating with the BWI Airport Authority on the best solution to ensure their operations are factored into the approved design for their international in-line system. Currently, TSA processes USTRANSCOM checked luggage at BWI using a lobby-based solution, which consists of screening checked luggage using Explosives Detection Systems (EDS) that are positioned at the ticket counter level of an airport, and requires manual labor to inject and remove bags through the EDS. Currently, TSA funds and staffs the resources required to process USTRANSCOM flights out of BWI.

TSA is committed to coordinating efforts between USTRANSCOM and the associated airport authority to efficiently use established resources.