AUTHORIZING THE TRANSPORTATION SECURITY ADMINISTRATION FOR FISCAL YEARS 2012 AND 2013

HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION SECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

JUNE 2, 2011 and JULY 12, 2011

Serial No. 112–28

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

72–238 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
PATRICK MEEHAN, Pennsylvania
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
MO BROOKS, Alabama

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
DANNY K. DAVIS, Illinois
BRIAN HIGGINS, New York
JACKIE SPEIER, California
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
KATHLEEN C. HOCHUL, New York
VACANCY

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*
KERRY ANN WATKINS, *Senior Policy Director*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON TRANSPORTATION SECURITY

MIKE ROGERS, Alabama, *Chairman*

DANIEL E. LUNGREN, California
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois, *Vice Chair*
MO BROOKS, Alabama
PETER T. KING, New York *(Ex Officio)*

SHEILA JACKSON LEE, Texas
DANNY K. DAVIS, Illinois
JACKIE SPEIER, California
CEDRIC L. RICHMOND, Louisiana
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

AMANDA PARIKH, *Staff Director*
NATALIE NIXON, *Deputy Chief Clerk*
THOMAS MCDANIELS, *Minority Subcommittee Director*

CONTENTS

AUTHORIZING THE TRANSPORTATION SECURITY ADMINISTRATION FOR FISCAL YEARS 2012 AND 2013

Thursday, June 2, 2011

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

The subcommittee met, pursuant to call, at 4:03 p.m., in Room 311, Cannon House Office Building, Hon. Mike Rogers [Chairman of the subcommittee] presiding.

Present: Representatives Rogers, Walberg, Cravaack, Jackson Lee, and Davis.

Mr. ROGERS. I would like to welcome everybody to this hearing and thank our witnesses for being here.

The purpose of this hearing is to discuss priorities for authorizing TSA to carry out its mission to keep America's transportation system safe from terrorists. This year, the committee plans to develop a TSA authorization bill which would enhance and streamline TSA's transportation security initiatives. For the record, Mr. Pistole, we are going to try to have that in July, early July, to develop that authorization bill.

TSA, like all organizations, has offices that could function more efficiently and effectively. It is the subcommittee's goal to improve TSA operations through oversight and legislation and to fulfill our responsibility to constituents by ensuring that taxpayer dollars are being spent in a cost-effective manner.

We appreciate the TSA's collaboration and input throughout this effort. Administrator Pistole, I agree with your vision for TSA, to develop a more risk-based approach toward passenger screening. A "trusted traveler" program would allow TSA to determine the level of threat posed by an individual and dedicate more resources to unknown or high-risk passengers.

I look forward to hearing an update on the status of the plan and the proposed parameters of a pilot or a larger-scale implementation. I hope TSA will consider this committee as a partner in the development and implementation of this type of passenger-screening reform.

Additionally, I hope to hear more about the priorities that we have discussed both publicly and privately, such as air cargo security, information sharing, and rail security initiatives.

Since the foiled Yemen cargo plot last October, TSA has been working with private industry to develop and implement short-

term security directives which seem to be successful in addressing certain vulnerabilities. However, no long-term plan has been formally outlined, and challenges remain.

In addition, the intelligence gathered from bin Laden's compound serves as notice that terrorists continue to target our surface transportation systems. Given the threats we face, it is critical that the resources that are available are spent effectively and with stakeholder input.

Mr. Pistole, I look forward to your testimony on this and other critical issues. I also want to highlight that the committee developed a TSA authorization bill last Congress, as well as H.R. 2200 under Ranking Member Jackson Lee's leadership. I look forward to working with her on a bipartisan basis throughout this effort.

Ms. Jackson Lee is on her way, and when she gets here, I will recognize her for a statement. But you are up, Mr. Pistole.

STATEMENT OF JOHN S. PISTOLE, ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. PISTOLE. Well, thank you, Chairman Rogers and Members of the committee. I appreciate the opportunity to be here today to discuss TSA's operations as you continue your important work in putting together a TSA authorization bill.

Much has happened since the last time I appeared before the subcommittee on February 10. Most significantly, Osama bin Laden is no longer with us. While his killing is significant, it does not, of course, mark the end of our effort to fight violent extremism. We have always known that the threat we face is bigger than any one person, just as we know that there are more terrorist groups plotting against us than al-Qaeda. So we remain vigilant in pursuing our vital mission of protecting the traveling public and safeguarding our Nation's transportation systems.

Since 9/11, together, we have implemented multiple layers of risk-based, intelligence-driven security measures: Dedicated transportation security officers, TSOs, continue working as the last line of defense; Federal air marshals patrolling the skies; behavior detection officers observing suspicious activity; mass transit and passenger rail security experts partnering with local authorities to deliver the tools they need to do their jobs; VIPR teams using K–9 assets to patrol all transportation venues, adding another layer of security against the terrorist threat. Our transportation security inspectors and other members of the TSA workforce continue to play their key roles in keeping us safe.

All of these individual measures, and others, combine to create a multilayered system of transportation security that mitigates risk. No measure on its own solves all of our challenges, but, in combination, they create a strong, formidable system. This is an approach with which you are intimately familiar. Indeed, your support for these operations has contributed immeasurably to their success.

I appreciate the opportunity to discuss with you ways to improve our existing efforts and to explore new and innovative techniques for Congress to consider in a TSA authorization bill, all in our current budget climate.

Now, two brief points regarding the budget. First, I am critically assessing TSA's operations at our headquarters level and in our field operations, with the goal of achieving efficiencies across the board. Second, the President's budget includes a $1.50-per-passenger fee which is critical to funding the security operations we employ to keep the over 1.7 million passengers safe and secure each day in the United States. I strongly urge this committee to support that fee, thereby saving taxpayers approximately $590 million in fiscal year 2012 alone.

Regarding risk-based security, since I became TSA administrator nearly a year ago, I have solicited ideas from people with diverse backgrounds and disciplines, from our dedicated workforce to our counterparts abroad, to airport and aviation executives and, of course, this subcommittee, about how TSA can work better. I have watched with great interest as specific proposals have been offered up by highly regarded voices in the security community.

As I stated previously, I believe that TSA must develop and implement smarter ways of performing its risk-based, intelligence-driven operations. If we can do that, we can move away from what seems to be a one-size-fits-all approach and stay ahead of the terrorists who are continually seeking new ways to undermine and defeat our security.

As we look for ways to evolve, we will move forward with a few fundamental principles—three principles. First, we must ensure than any new step we take strengthens security. Second, we must recognize that the vast majority of the hundreds of millions of people who use our transportation systems every year present little to perhaps no risk of committing an act of terrorism. Then, third, while we can mitigate risk, we must be honest with ourselves and the public in acknowledging that we will never fully eliminate all risk.

With these principles in mind, we have been exploring ways we can get smarter, improve security, and enhance the travel experience for most people. For many, a change in TSA's approach cannot come soon enough, and the proof will be in how any changes are designed and implemented. We all wish it were simple and that we could make significant changes tomorrow, but you know as well as I that that is not the case. So while we pursue a new approach to passenger screening, we still have a job to do today.

I would like to take a moment to thank the transportation security officers and all the men and women of TSA, who continue to faithfully and diligently perform their duties in the face of negative reporting and even efforts to criminalize their jobs. Effective TSOs result in effective security, both today and in the future. So this will be an on-going collaborative effort.

In the nearly 10 years since 9/11, we have done important work to keep the travelling public safe with this committee's support. So I look forward to building on our already-strong relationship as we continue, together, to work to improve security in the next decade. Thank you for your support and constructive engagement.

[The statement of Mr. Pistole follows:]

PREPARED STATEMENT OF JOHN S. PISTOLE

JUNE 2, 2011

Good afternoon Chairman Rogers, Ranking Member Jackson Lee, and distinguished Members of the subcommittee. We appreciate the opportunity to appear before you today as the subcommittee begins consideration of a Transportation Security Administration (TSA) authorization bill.

TSA employs risk-based, intelligence-driven operations to prevent terrorist attacks and to reduce the vulnerability of the Nation's transportation system to terrorism. Our goal at all times is to maximize transportation security to stay ahead of the evolving terrorist threat while protecting passengers' privacy and facilitating the flow of legitimate commerce. TSA works collaboratively with industry partners to develop and implement programs that promote commerce while enhancing security and mitigating the risk to our Nation's transportation system. We also work closely with other Federal agencies and maximize participation from State, local, Tribal, and private sector stakeholders to work toward a common goal of securing all modes of transportation, including aviation and surface transportation systems.

TSA has implemented an effective and dynamic security system in the aviation domain consisting of multiple layers of risk-based measures. In the aviation arena, our security approach begins well in advance of a traveler's arrival at an airport, with our vetting programs and intelligence analysts, cargo and compliance inspectors ensuring that airport security plans are followed, and our law enforcement and intelligence community partners working to detect, deter, and prevent terrorist plots before they happen. The security system continues at the airport, including, but not limited to, the work of our Behavior Detection Officers (BDO); Transportation Security Officers (TSO) and the technology that supports the screening of passengers and baggage; Bomb Appraisal Officers (BAO); and canine teams, as well as our partnerships with local law enforcement. In flight, thousands of Federal Air Marshals (FAM) and Federal Flight Deck Officers (FFDO) protect the traveling public. The traveling public also plays an integral part role in the security system. For example, the DHS "If You See Something, Say Something" campaign engages the public and key frontline employees to identify and report indicators of terrorism, crime, and other threats to the proper transportation and law enforcement authorities.

In the surface transportation arena, we continue to work with our law enforcement and security partners to reduce vulnerabilities and strengthen resilience against a terrorist attack. TSA works with the Federal Emergency Management Agency Grants Program Directorate to direct Federal grants to the most at-risk transit properties. Our Surface Transportation Security Inspectors assist with the development of specific security programs. Our Visible Intermodal Prevention and Response (VIPR) teams are deployed on thousands of mass transit, pipeline, maritime, and highway missions annually to enhance security, provide deterrent and detection capabilities, and introduce an element of unpredictability in security practices and procedures in order to prevent or disrupt potential terrorist planning activities.

TSA also conducts protection, response, detection, and assessment activities in airports and other transportation systems; trains and manages all armed pilots; and coordinates all TSA canine assets. Our personnel are continually adjusting and adapting security practices and procedures to best address evolving threats and vulnerabilities, and disrupt the ability of terrorists to plan and execute attacks.

TSA SECURITY OPERATIONS AND TECHNOLOGY DEPLOYMENTS

TSA works diligently to protect the U.S. transportation domain against evolving threats to security. We continue to modernize our technology, including Advanced Imaging Technology (AIT). We have deployed nearly 500 AIT machines at domestic airports throughout the country to enhance security by safely screening passengers for metallic and non-metallic weapons and explosives—including objects concealed under layers of clothing, while protecting the privacy of the traveler. We will procure and deploy an additional 500 AIT units using fiscal year 2011 funds for a total of 1,000 AIT units, which will allow us to screen an estimated 60 percent of passengers using this technology. We have also deployed new portable explosive trace detection machines, Advanced Technology X-ray systems, and bottled liquid scanners to enhance our security technology in the aviation domain. This suite of technologies represents the most effective means of detecting current threats available today.

In order to continue the deployment of this critical layer of security, the President's fiscal year 2012 budget request includes $105.2 million in base and additional funding to deploy and staff 275 additional AIT units, bringing total coverage to

1,275 AITs by the end of 2012 and providing coverage to 80 percent of passengers. Congressional funding directly affects our ability to deploy this critical technology.

While we are rapidly deploying AIT machines to U.S. airports, we also are exploring enhancements to privacy protections and operational utility. Specifically, TSA has field tested auto-detection software for AIT machines, referred to as Automatic Target Recognition (ATR). ATR eliminates passenger-specific images of a passenger and instead highlights a detected anomaly on a generic outline of a person. Pat-downs used to resolve such anomalies are limited to the areas of the body displaying an alarm unless the number of anomalies detected requires a full-body pat down. If no anomalies are detected, the screen displays the word "OK" with no icon. With ATR, the screen will be located on the outside of the machine and can be viewed by the TSO and the passenger.

As with current AIT software, ATR-enabled units deployed at airports are not capable of storing or printing images. The ATR software eliminates the need for a TSO to view passenger images in a separate room because no visual image of the passenger is produced, reducing associated staffing and construction costs. ATR software represents a substantial step forward in addressing passenger privacy concerns, while maintaining TSA's standards for detection. TSA plans to continually update and test enhanced versions of the software in order to ensure that technology with the highest detection standards is in use.

In addition to deploying the most effective technology, we have also deployed additional BDOs, FAMs, and explosives-detection canine teams at airports throughout the country. We have implemented security measures for all air carriers with international flights to the United States that use real-time, threat-based intelligence to better mitigate the evolving terrorist threat. Last November, we achieved a major aviation security milestone: 100 percent of passengers on flights within, departing from, or bound for the United States are now checked by TSA against Government watch lists through the Secure Flight Program, as recommended in the *9/11 Commission Report.* Continuous Secure Flight vetting begins 72 hours in advance of flight and continues until the flight departs, consistently providing insight into potential threats and enabling TSA and our law enforcement partners to counter these threats accordingly.

State Laws That Could Adversely Impact AIT Deployment

It is fitting that, as this subcommittee considers new authorizing legislation for TSA, we address an issue that has recently received some media attention. Since the deployment of AIT and the implementation of our revised pat-down procedures at airport checkpoints Nation-wide to better detect prohibited items and resolve anomalies that are detected on passengers, some State legislatures have introduced legislation that would ban AIT units and even criminalize certain TSA pat-down procedures. It is TSA's position that, since TSA is a Federal agency, individual States are preempted from interfering with the deployment of TSA personnel and equipment in carrying out statutorily mandated security programs that are necessary to keep our aviation security system strong and safe for the traveling public. It is also important for our workforce to know TSA will stand by them as they execute their important responsibilities. State law proposals that would attempt to restrict cooperation between airport authorities and TSA in performing security measures diminish aviation security and leave the aviation system more vulnerable to a real and continuing terrorist threat.

SURFACE TRANSPORTATION SECURITY

TSA's efforts in the surface transportation domain are undertaken to reduce security vulnerabilities and to strengthen resilience against a terrorist attack. TSA works with its partners to secure and safeguard the surface transportation domain—which includes subways, bus transit systems, ferries, pipelines, the National Railroad Passenger Corporation (AMTRAK), commuter railroads, and freight railroads, among others—through a variety of programs. Many of these programs enhance security by addressing policy gaps and obstacles, enhancing coordination and unity of effort, and maximizing the strengths and capabilities of our partners, keeping with the themes that guided the March 2010 Surface Transportation Security Priority Assessment.

Because mass transit and passenger rail systems serve large populations in major metropolitan areas, many with substantial underground infrastructure, bridges, and transportation staging areas, or hubs, which can include other forms of transportation, these systems remain a target for terrorist groups. The characteristics essential to mass transit and passenger rail—i.e., an inherently open architecture moving large populations in major metropolitan areas through multimodal systems and infrastructure—create potential security vulnerabilities. TSA uses a collaborative ap-

proach—working with State and local law enforcement and transit authorities—to assess risks and enhance security.

TSA's role in surface transportation security involves direct engagement with surface transportation owners and operators to establish security standards, provide grant funding, share current risk information and assess security measures. For example, TSA uses the Transportation Systems Sector Risk Assessment to evaluate threat, vulnerability, and consequence in a wide range of terrorist attack scenarios for each mode of transportation. To help address the results of these assessments, the Department of Homeland Security's (DHS) Transit Security Grant Program (TSGP) provides awards to eligible transit agencies to assist State and local governments in devising and implementing initiatives to improve security. The TSGP promotes a sustainable, risk-based effort to protect critical surface transportation infrastructure and the traveling public from acts of terrorism. In 2011, DHS announced a new model for TSGP to focus limited resources on "shovel-ready" projects hardening the highest-risk transit infrastructure, while prioritizing operational deterrence activities such as training, exercises, canine, and mobile screening teams.

TSA also currently operates 25 VIPR teams across the transportation sector, and the fiscal year 2012 budget request includes funding for 12 additional multi-modal VIPR teams. These teams consist of personnel with expertise in inspection, behavior detection, security screening, and law enforcement for random, unpredictable deployments throughout the transportation sector to deter potential terrorist acts. There have been more than 3,000 VIPR operations in the current fiscal year, 70 percent of which occurred in the surface transportation sector.

In addition, structural vulnerability assessments are currently being conducted on the Nation's most critical highway, bridge, and tunnel infrastructure. These assessments, performed for TSA by the U.S. Army Corps of Engineers, are the most comprehensive assessments that have ever been performed. Additional assessment visits are also taking place at the State level and in conjunction with the companies that transport goods and passengers across the country. Finally, TSA is delivering security awareness training to the highway transport community; more than 200,000 individuals have been trained by the TSA-directed "First Observer™" program and similar TSA-sponsored training. Further, in response to a strong demand, TSA has distributed counterterrorism guides throughout the trucking, motor coach, school transportation, and infrastructure community.

Air Cargo Security

TSA has and will continue to focus air cargo resources to ensure continued compliance domestically with the 100 percent screening requirement, and to work toward further risk-based screening of international inbound air cargo on passenger and all-cargo aircraft. Along with its participation in the DHS Air Cargo Security Working Group established by Secretary Napolitano, TSA is continuing its leadership role in partnering with industry and other Federal Government partners to develop strategies to strengthen air cargo security while facilitating the flow of commerce. In January 2011, TSA issued proposed air carrier security program changes to increase security measures for air cargo, most notably, to require 100 percent screening for inbound international air cargo transported on passenger aircraft by the end of this calendar year. TSA is currently finalizing its analysis of industry comments. TSA is also working closely with U.S. Customs and Border Protection and the air cargo industry to receive and process pre-departure, advanced air cargo information about shippers earlier than is currently required so that we can increase the focus of our screening resources on high-threat cargo. TSA will also continue its efforts to test, evaluate, and qualify air cargo screening technologies.

TSA EXPLOSIVE DETECTION INITIATIVES

TSA continually seeks to enhance capabilities for explosives detection as part of its risk-based and intelligence-driven strategy. To enhance our application and deployment of explosive detection canines, TSA partners with academic, research, and professional organizations with the appropriate research capabilities to develop, explore, and implement emerging explosive detection methodologies that have been subjected to extensive, rigorous research and testing. Further, TSA works with these organizations to determine how to harness these methodologies to gain the maximum explosives detection efficiency in the transportation system.

Last January, TSA, in partnership with the DHS Science and Technology Directorate, initiated a pilot program to evaluate 10 air scenting explosives detection canine teams, utilizing the methodology developed by Auburn University known as "vapor wake" explosives detection. The methodology relies on the canine's ability to process air currents and recognize odors that it is trained to detect, whether the scent emanates from a person who is moving or standing still, or an inanimate ob-

ject. Neither the canine nor the handler needs to come into direct physical contact with a person who may be a potential target—in fact, the canines can detect a scent even if the potential threat has left the immediate area and track the scent to its current location. A major advantage of this methodology is that the handler is trained to read the canine's behavioral changes to determine when and where the canine is alerting to an explosives odor, on a subject, without the knowledge of the targeted subject.

A RISK-BASED STRATEGY FOR THE FUTURE

TSA's existing security measures create a multi-layered system of transportation security that mitigates risk. No layer on its own solves all our challenges, but, in combination, they create a strong and formidable system. In the months ahead, I am optimistic that we will be able to brief this subcommittee and others in Congress about some initial steps we are taking to further enhance security by becoming even more risk-based in our approach to aviation security.

As our risk-based approach evolves, we must ensure that each new step we take strengthens security. Since the vast majority of the 628 million annual air travelers present little to no risk of committing an act of terrorism, we should focus on those who present the greatest risk, thereby improving security and the travel experience for everyone else. Since I became TSA Administrator a year ago, I have listened to ideas from people all over the world, from our dedicated workforce to our counterparts abroad, about how TSA can work better and smarter. Last fall I directed the agency to explore ways to develop a strategy for truly risk-based security. That strategy will examine the procedures and technologies we use, how specific security procedures are carried out, and how screening is conducted. While TSA currently implements a risk-based security system, we must continue to assess our programs to evolve our security approach to stay ahead of tomorrow's security threats.

To that end, we are working to expand our ability to conduct more identity-based screening. This is evident in our work on a new crewmember screening system. We are currently testing an identity-based system to enable TSA security officers to positively verify the identity and employment status of pilots. We hold pilots responsible for the safety of the traveling public every time they fly a plane. It just makes sense to treat them as trusted partners, as well.

While the initial iteration of this risk-based screening focuses on pilots, we are also looking at long-term concepts to focus limited resources on higher-risk passengers, while expediting and enhancing the passenger experience at the airports whenever possible. This will be an on-going, collaborative effort with law enforcement, airport authorities, and the traveling public. As our risk-based screening evolves, we will continue to incorporate random security steps as well as other measures both seen and unseen.

2011 AUTHORIZATION BILL

As the subcommittee considers a TSA authorization bill, two issues that deserve close consideration include the following:

Aviation Security Service Fee

Since its establishment in 2001 as part of the Aviation and Transportation Security Act, the Passenger Civil Aviation Security Service Fee has been limited to $2.50 per passenger enplanement with a maximum fee of $5.00 per one-way trip and has not been adjusted for inflation or the increased costs of providing security over the past 9 years. Despite Congress's original intent that the security fee cover nearly all costs related to passenger and property screening, the fee currently offsets less than a third of the total cost of aviation security. At the same time, costs of security have continued to increase. In fiscal year 2010, the average cost for the TSA to screen a passenger and baggage was nearly $9; in 2000, the cost was less than a dollar per passenger.

We ask that the subcommittee give serious consideration to the President's fiscal year 2012 budget proposal to permit DHS/TSA to gradually increase the Passenger Civil Aviation Security Service Fee. This adjustment will ensure that we are able to continue the significant progress we have made in enhancing aviation security while fulfilling Congress' intent to do so in a fiscally responsible manner that does not penalize American taxpayers.

Procuring and Installing EDS Equipment with ASCF Funding

As you know, current law requires the first $250 million derived from passenger and air carrier security fees in fiscal years 2004 through 2028 to be deposited in an Aviation Security Capital Fund (ASCF).

The ASCF is distributed to airports through grants for airport security capital improvement projects. These projects typically include facility modifications, design and build-out for integrated baggage handling, and Explosives Detection Systems (EDS). These grants cannot be used for the procurement and installation of the actual explosives detection equipment that these modifications are designed to accommodate, however, because TSA, and not the airports who receive these grants, is responsible for the procurement and installation of that equipment.

TSA has already funded, or is currently funding, most of the projects eligible for ASCF funding and does not expect applications for many new eligible projects in the foreseeable future. A critical need exists, on the other hand, for TSA to procure and install large quantities of the EDS equipment itself, in order to replace aging and less up-to-date security technologies. TSA currently has approximately 2,000 EDS units deployed Nation-wide. By 2013, almost half of those units will have reached the end of the anticipated useful life of 10 years. Because the EDS equipment is an integral part of the projects Congress intended to fund with the ASCF, we ask this subcommittee to give serious consideration to correcting this situation by adopting a provision to permit the ASCF to be used for the procurement and installation of EDS equipment.

Additionally, current law requires TSA to issue letters of intent (LOI), which are agreements to provide funding over a period of several years. Again, the major projects for which such funding would be appropriate have already been funded. On the other hand, there is a need to fund smaller capital projects through single-year funding. We request this subcommittee consider amending the law to permit use of the ASCF in this manner. With these two amendments to the ASCF language, TSA could more effectively, efficiently, and expeditiously plan and implement the necessary acquisition and replacement of existing EDS units, and provide funding to airports for smaller capital aviation security projects that do not require multi-year funding.

CONCLUSION

I want to thank the subcommittee for its continued assistance to TSA and for the opportunity to discuss our programs as the subcommittee initiates its work on a TSA authorization bill. I am pleased to answer any questions you might have.

Mr. ROGERS. I thank you.

We will go ahead and move to questions. I do want to go ahead and let you know that we are probably going to be called for votes around 4:45, 4:50, somewhere in there. So we are going to try to move this along and get as much in the record as we can.

First thing, as you know, I am very interested in the known-traveler program and doing some things to focus our limited resources on the real threat-based risk. What I would like for you to do is give us a report on the status of the development and implementation of that known-traveler program. Some people call it the "trusted traveler" program, but whatever.

Mr. PISTOLE. Thank you, Mr. Chairman. Yes, some people refer to a "trusted traveler," which may imply that everybody else is not trusted, and some people refer to "known." Whatever we call it, we look at it as a risk-based security initiative within TSA and the Department of Homeland Security where we can focus our limited resources on those that we know the least about, who may cause us the most problem.

So the idea is, in very general terms, that those people willing to share information with us about their travel histories, their travel patterns, perhaps what is in their frequent-flyer account, that we can make informed judgments about them that may expedite their security screening.

That may look different at our 450 airports around the country, just because of the checkpoint configuration. But the idea would be to allow that person who has shared information with us, that we

can make an informed judgment about, that that person would be allowed to be expedited in how they are physically screened.

The first example that we have of this is with the actual pilots of the aircraft that we are trying to finalize. We are in the process of finalizing the system with the airline associations and the pilot associations to do an identity-based screening for them. We also are working with the Flight Attendants Association to do the same thing with them, after the pilots' program is working, because they are the most known and trusted—the pilots and then the flight crews.

As we work through those that we know more about, then we can make similar judgments, allowing us to improve security, I believe, by focusing on those that we don't know much about. Obviously, in Secure Flight, we know the three data fields—name, date of birth, and gender—which allows us to determine whether somebody is on a watch list or not, but it does not really give us much more information.

Again, for those who are willing to share information with us, then we will work through that to provide that streamlined processing, using more intelligence on the front end, more identity-based, and, frankly, getting away from some of the physical screening that we have come to be known for in doing our thorough security.

There is a lot more to it, but that is where we are now. We hope to be doing some more testing this summer, doing some education and training for our workforce on how this would look. Then in the fall, we hope to try some pilot projects on this in certain airports and just see what it would look like, recognizing, again, that some airports may be able to have a dedicated lane for these people who are in the known- or trusted-traveler program, but it would not be the same in every airport. So we need to manage expectations with the traveling public.

The one thing I would say, Mr. Chairman, is that it would not be a program that people would pay a fee to join, a program such as Global Entry. But people in Global Entry, for example, where we already know a lot about them, would be part of this known group. They have already submitted to a background, they have been interviewed and things like that. There are other groups of people, obviously, those both in the private sector, the public sector, people with Top Secret security clearances, any number of people that we can look at and—a lot more detail, but that is it in a nutshell.

Mr. ROGERS. All right. So, the pilot programs by the end of this summer. Then what time line do you think you will be able to take the lessons learned and incorporate that into a more global——

Mr. PISTOLE. So, actually, we would do the internal work this summer, in terms of enhanced behavior detection work and training our workforce in how would they handle these people, because there are a lot of issues in terms of the hand-off and who goes where for what. So we will spend the summer making sure that is working.

So we are actually looking at the fall of doing these trial efforts in several airports, working with several airlines. So we are really

looking at this fall for that and then much more expanded as we go into 2012.

Mr. ROGERS. Great.

I wanted to ask you a little bit about an update on the air cargo aircraft after the Yemen terrorist attack. What kind of modifications have you made to prepare precautions for that kind of attack again?

Mr. PISTOLE. So, since the Yemen cargo plot of October 28 and 29 of last year, we have worked very closely with industry, in terms of coming up with, again, a risk-based approach to what makes sense that they can provide, we and they and host countries can provide, the best possible screening for those unknown shippers or unknown shipments. Those are the two criteria that we are looking at.

So, as opposed to having just an across-the-board rule that says, this will be the same screening for every package, every piece of cargo, every piece of mail that goes in passenger planes and things, we are trying to tailor it. Having some great work by industry, FedEx and UPS domestically, DHL, other cargo carriers, working very closely with us to implement and effect those changes that provide for better security so we will have the best intelligence-based reasons for doing screening, as opposed to just a blanket screening protocol across the board.

Mr. ROGERS. Great. Thank you.

My time has expired. I now recognize the gentleman from Minnesota, Mr. Cravaack, for 5 minutes.

Mr. CRAVAACK. Thank you, Mr. Chairman.

Thank you. I appreciate you coming here today and advising us about this very important aspect of our National security.

Sir, in your written testimony, you mention that the TSA is rapidly deploying AIT machines to the U.S. airports and exploring enhancements to the privacy protections. Do you have a time line for how long this is going to take, to fully fit all the AIT machines with automatic target recognition software that would eliminate passenger-specific images from being generated during the TSA screening?

Mr. PISTOLE. Yes, Congressman Cravaack. Thank you.

We have approximately half of our nearly 500 machines out there right now, which have the capability for being upgraded, if you will, to the automatic target recognition. We have done pilot work in three airports—Atlanta, Las Vegas, and Reagan National—with good success. So, by that, I mean, our expected rates, in terms of detection and false positives and throughput, some of the basic criteria, have all been positive.

So, for half of those machines, so about 240-plus, the plan is, assuming a couple more things are done in the next week or 2, that we would modify those throughout the rest of this year, the calendar year, 2011.

The other manufacturer that has not quite developed that protocol with the software and the depiction of the generic outline of a person, we are doing lab testing over the next couple months and hope to field-test their software in the fall and, assuming everything goes well, follow very shortly with the rest of those machines, which, as you noted, completely address, I believe, the privacy

issues because there is not an image of a person, it is just a generic outline of a person, with an area of any anomalies highlighted.

So that is where we are.

Mr. CRAVAACK. Okay. Thank you, sir, on that one.

The other thing I have is a question in regards to—the complaints that I hear from the majority of people that I speak with regarding TSA usually are person-to-person type of issues, going through the checkpoints, things like that. What kind of standardization process—I mean, and I experience—obviously, I am on the road quite a bit. I experience it, myself. I have to take off my belt, at this station, at this city, sometimes. I was wondering, how can you address the standardization issue?

The other aspect is, your personnel that work at these checkpoints, do they get training on how to basically interact with the public? You see some stations that are extremely professional, and then you have other stations that look like a bunch of high schoolers having a fun day on a break. Could you comment on that?

Mr. PISTOLE. So, on the standardization issue, part of it may be driven by whether they have the advanced imaging technology, which does require a belt to come off and everything to come out of pockets, whereas—and we have that in 75 airports or so. I will have to check on that, the exact number. So if they just have to walk-through metal detectors, you probably don't have to take your belt off unless it has a large metal buckle or something like that, but typically not. So that is one issue.

In terms of the training, every new TSO goes through training in terms of, not only as a security apparatus and protocols, but in customer service. Some, as you note, do it better than others. We try to do retraining for those that we have issues with or that people have complained about, basically. Then, if appropriate, we take disciplinary action if it rises to a level of unprofessionalism as opposed to just not being good customer service.

The bottom line is, we tell them to focus on the security aspects, but the better they can engage a passenger, you know, the 1.7 million every day—the vast majority are positive. I do receive some positive comments, from time to time, from passengers who get my e-mail or something. But those that we learn about are often the ones that have not been the most positive.

Mr. CRAVAACK. I appreciate that. Just to clarify, what I was talking about was going, actually, through the scanners themselves. Some places, I do; some places, I don't. Being a part of this committee, it just adds a little bit of a question mark in my mind, what is the proper standardization? Being an old Navy pilot, standardization is the key, and so I just wanted to comment on that.

But, otherwise, sir, thank you for everything that you do. Thank you for all the great TSA agents that do their job exceptionally well every day.

With that 10 seconds, sir, I will yield back.

Mr. PISTOLE. Thank you for your support, Congressman.

Mr. ROGERS. I thank the gentleman.

I would love to have seen the investigation into who leaked your e-mail address in-house. I bet it was vigorous.

The gentleman from Illinois, Mr. Davis, is recognized for 5 minutes.

Mr. DAVIS. Thank you very much, Mr. Chairman.

Mr. Pistole, let me turn to another area. I would like to turn to the rulemaking for frontline surface employee training and security assessments, which are required by the 9/11 Act. These regulations are more than 2 years overdue. Can you tell us what has been causing the delay in getting these rules done?

I ask because the scope of the rulemaking will determine the amount of surface inspectors required for both regulatory and industry stakeholder consultation purposes. So I would appreciate knowing what is holding that up.

Mr. PISTOLE. So, just to clarify, Congressman, the rulemaking as it relates to—what was the specific area?

Mr. DAVIS. Rulemaking, training, and security assessments.

Mr. PISTOLE. So, if I understand the question, in terms of our surface transportation inspectors, is that where you are focusing?

Mr. DAVIS. Right.

Mr. PISTOLE. Okay. So there has been a lot of work done in terms of a workforce assessment. Then I am, frankly, not quite sure on the rulemaking as it relates to that, so I will have to get back with you on that. I am not following exactly what that is.

But I would be glad to talk about the surface inspector program, in general, and the training with that, if that is what you are——

Mr. DAVIS. Yeah.

Mr. PISTOLE. Okay. So, as you know, we have nearly 2,000 inspectors overall, some in aviation, some cargo, about 400 or so in surface, 120 in K–9 cargo, 84 international inspectors. The surface inspectors, of course, do much in the area of rail, both passenger and freight rail, in terms of working with the industry to assess vulnerabilities.

One of the key areas of success has been in terms of the toxic inhalation hazard and working, in a voluntary way, with industry, where we identified some vulnerabilities and gaps through what is known as BASE, which is a baseline assessment security evaluation. Because of those vulnerability assessments, industry, on their own, decided to make some changes in the way that railcars with toxic gases and things, where they sat overnight, for example, or how much time they spent, for example, going through downtown Washington, DC, and could they re-route and things like that.

So industry actually made a number of substantial changes that reduced the risk 50 percent in the last 2 years and over 90 percent in the last 5 years, without regulation. So it is that type of partnership that we are looking for with industry to address those issues.

Mr. DAVIS. All right.

Let me ask you, regarding the new grant guidance that was released by the Department last month, a revised risk formula will be used when considering applicants.

My question is twofold: What was TSA's role in developing the new grant guidance with other Department components and stakeholders? Second, how do you anticipate this new grant guidance will impact mass transit agencies across the country?

Mr. PISTOLE. The TSA's role in the development of the guidance was to work closely, particularly with FEMA and with the Department of Homeland Security, to look at a couple of broad areas.

One is, do we take these funds and try to spread them out across the country, even including areas that have not been identified as high-risk and try to do what some people describe as a peanut-butter approach: Do we just spread it out evenly across the country without regard to risk?

Or, my preference was, and is, that we look at what the intelligence tells us to be a risk-based organization and say, let's focus our money that is administered through FEMA in areas that we know are the greatest risk, so whether it is Chicago, whether it is New York, the District of Columbia, Los Angeles. My hometown in central Indiana is a great hometown, but it has never once come up in the threat matrix. So it is just something that—the idea is, how can we use our money intelligently to augment and enhance those efforts?

So that is our role in it. As it relates to mass transit, the idea is to provide those funds to those mass transit components, such as the New York transit system with over 5 million passengers every day in the subway; Chicago, obviously the L and the Chicago Transit Authority, a lesser number. But, still, those are higher-risk areas. So that is the approach.

Mr. DAVIS. Thank you very much.

Thank you, Mr. Chairman.

Mr. ROGERS. I thank you.

The Chairman now recognizes the gentleman from Michigan, Mr. Walberg, for 5 minutes.

Mr. WALBERG. Thank you, Mr. Chairman.

Thank you, Mr. Pistole, for being here with us today. Thank you for the work you do. Thankless, in many cases, but so necessary.

I don't like going through AITs. It is not because of the laughter as I am standing on the yellow footprints. But it certainly takes some time, it takes additional support staff, TSA staff there. It is discretionary to some point and not always objective, it appears. But it is what it is.

My question is: There are other technologies that are out there, some that are being used to ascertain explosives, drugs, you name it, used by other entities, including the DOD. Are there any of those technologies that you are looking at that would supplement and/or replace AIT-type machines, including the nonspecific image, which would be great to get, but, as an alternative to that, something that is being used effectively in a field situation now and with a high degree of certainty? Are you entertaining those?

Mr. PISTOLE. Yes, Congressman.

Let me apologize for the laughter up front. That should not be the case, if that ever is.

So——

Mr. WALBERG. You don't know me.

Mr. PISTOLE. So, I view AIT, the advanced imaging technology, as the best technology we have at present to detect the non-metallic-type device that we saw on Christmas day 2009, where, you know, we have something that if somebody walks through a walk-

through metal detector and doesn't alarm at all because there is no metal in that improvised explosive devise.

That being said, it is not a panacea, it is not a silver bullet. It is one of the tools we have. Other tools that we have are explosives trace detection, whether it is on the hands for somebody, whether it is on a bag in case there are explosives in the bag. The use of K–9s—we use and we are wanting to use more of the vapor-wake dogs that can pick up the scent, if you will, the molecules of explosives even though they don't hit on the bag itself. If the bag has gone by, whether it is a backpack or whatever else, like we saw with the July 7, 2005, bombers going into the London Tube. So we are interested in all those, along with behavior detection, along with all those other things.

One of the things—the AIT and now the automatic target recognition is actually increasing the throughput; we are getting people through more quickly. But I would just note that, because of the increased carry-on bags that people—I am sure you have never done this. But in carry-on bags, people are jamming a lot of things in there so they don't have to pay a fee for some airlines with a checked bag. The denser the bag, then the more challenging it is for our security officers looking at the X-ray to say is there something bad in there. So, actually, we are finding that is taking longer, to resolve those issues, than it is for the passenger themselves.

Just as an example, in the last 2 years, we have gone from about 1.25 million carry-on bags every day that we screen to 2½ million. It has literally doubled. So you think of that in terms of what the security officers are trying to look at.

If you haven't seen the demonstration of what we actually do, I would encourage you to do that. Because when I saw what the security officers are looking at on the screen in trying to discern, this is a bad item, this is okay, it is very difficult. So I have a great deal of respect for these officers who do that.

Those are some of the technologies, but we are always looking for other opportunities. We do work with DOD, we work with DARPA, in terms of some of the cutting-edge technologies that haven't been proven yet. What I want to make sure, though, is we are using taxpayers' dollars in a wise way to get to the best technology as one of the many layers of defense.

Mr. WALBERG. Well, I would encourage that, because if the figures are correct that you give us, that we have gone from less than a dollar to now $9 per passenger, on average, to screen people since 2000—and we understand the main reasons for that. But there certainly has to be ways that we can speed up, do very accurate, and get away from that challenge of what you are saying is inside the bags right now.

You know, I have been told that there are passive-screen effective modes right now that are being used by DOD, in extreme situations, that would be used on every passenger, no one getting by that, and yet would be less intrusive and maybe even quicker. So I certainly would encourage that.

Mr. PISTOLE. Thank you. Yeah, I am very much interested in that, and I will follow up with DOD on that.

Mr. WALBERG. Thank you.

Mr. ROGERS. Great. I appreciate that.

I want to go back to the air cargo issue we were talking about at the end of my last section of questions. You know, we have had a lot of discussion in this committee and the full committee over the years that I have been a Member about the need to achieve 100 percent screening of all cargo, not just on domestic passenger planes but passenger planes that are inbound from foreign countries and for domestic cargo planes.

There has been a lot of discussion about the fact that they just don't think that, from a technical standpoint, it is feasible to achieve 100 percent. What are your thoughts on what is do-able in the area of air cargo?

Mr. PISTOLE. I think we can achieve a high level of screening and performance with those highest-risk packages. In dealing with industry, really since the Yemen cargo plot of late October last year, what we have learned is that to do a piece-by-piece screening of each item of cargo or, say, mail parcels over 500 grams, whatever it may be, would really shut down the global supply chain, which we have no interest in doing.

What we are interested in doing is working with industry and, frankly, with CBP, Customs and Border Protection, in terms of advanced information about packages, particularly coming from overseas, from what may be determined to be high-risk areas, those that we assess that the screening is not as thorough as it is here in the United States, the concern, obviously, being for cargo and those parcels that end up on passenger planes. As we know, the majority of cargo does end up on passenger planes.

So what additional scrutiny can be applied to those from the two criteria of, is it a known shipper—that is, does the shipper have a business relationship with the carrier, with the shipper; and then, is it a known shipment, meaning is it something that is just coming in over the counter—for example, the Yemen cargo plot, where the one young woman comes in. She is completely covered, other than her eyes. She presents the package with the toner cartridge, the two packages. She gives a false identity, false ID. The freight forwarder there that forwarded it on to Dubai did what they were supposed to do at that time, just do a physical inspection. "Yeah, it is a printer and some clothing, and so we will go ahead and ship it."

What we have done with industry and what they have done on their own is to develop some rule-based protocols to say, does this make sense, that somebody is paying $500 to ship a computer printer and some books and clothes from Sanaa, Yemen, to Chicago? Does that make any sense? So it is that combination of getting advanced information, similar to the API, the advanced passenger information, passenger name records, that construct, for cargo.

So, to answer to your question succinctly, I think we can achieve a high percentage of cargo coming to the United States. But to get to 100 percent with any confidence would require substantial additional resources for us to not only trust but verify——

Mr. ROGERS. Right.

Mr. PISTOLE [continuing]. What is happening on the ground in all those last points of departure around the world.

Mr. ROGERS. That is my concern. I think if you are going to use some sort of technology to screen, as opposed to the K–9 detection that I support, as you know, I just don't know how we would ever afford the kind of infrastructure we would have to have just for the domestic cargo, not to mention the in-bound foreign flights.

But I want to go back to your opening statement. You made reference to the fact that you do want to see us move to a more risk-based approach. How can the Congress, how can this committee in this reauthorization, how can the Congress help you achieve that change in the way you focus your energies and resources?

Mr. PISTOLE. Thank you, Chairman.

Before I answer that, if I could just—one more point on cargo. We work with countries to develop National cargo screening programs, so we can recognize the country's program, similar to what we do here in the United States, to address that, so we are not actually out there inspecting at each last point of departure.

On the risk-based security, I think the best way for this subcommittee and committee and the Congress as a whole is to provide us your ideas, your thoughts, about what works best from both a security standpoint but also from the—what makes good business sense, and as we talk about some of these ideas further, to work with us in a collaborative fashion.

I don't think—one of the beauties of this proposal that we are pushing is that, right now, there is no rulemaking that is required, there are no fees required, there is no legislation that is required. So, at least in the initial iteration, it is simply to have your support as we move forward on this.

As we engage industry, we are getting very positive feedback. So I think we are on the right track. But I do want to manage expectations and, frankly, under-promise and over-deliver as we move forward.

Mr. ROGERS. Well, the reason I ask is, as you know, we are about to draw up an authorization bill. I would like particularly the intelligence segment of your organization to be thinking, is there going to be some sort of authority that we are going to need from the Congress to do something different?

Mr. PISTOLE. Okay.

Mr. ROGERS. It is just, this is the time to be thinking about any language——

Mr. PISTOLE. Yes.

Mr. ROGERS [continuing]. And not next year, when we have already——

Mr. PISTOLE. Right.

Mr. ROGERS. So, anyway, that is all I am asking for.

I am thrilled to announce that my good friend from Texas, who has been over at the White House with the President, has been able to make it back before the end of the hearing. I don't know if she wants to offer a statement or just go to questions. But she is occupied right now.

Do you want to offer a statement or go straight to questions?

Ms. JACKSON LEE. No, I would like to——

Mr. ROGERS. Wait? Okay.

Mr. Cravaack of Minnesota is recognized.

Mr. CRAVAACK. Thank you, Mr. Chairman.

Just to kind of dovetail a little bit about what you were talking about earlier, sir, being an airline pilot, I was just wondering if you can elaborate a little bit about the known-crew-member program and when you feel like it will be fully implemented?

Mr. PISTOLE. We have tested this through what is known as "Crew Pass" in three airports—Pittsburgh, BWI, and Columbia, South Carolina—with good success, in terms of having the technology at the checkpoint where the pilots literally go through an identity-based screening. The key for us is making sure that we have that technology available at each checkpoint, particularly the 28 Category X airports and the Cat 1 airports, the largest airports, where the greatest number of pilots are going through.

I have actually approved the policy. It is simply a matter of working out the technology end of it between, again, the pilots associations and the airlines. So they are working through that.

My only requirement is that we have one common system. I am agnostic as to what company or anything like that. But as long as we can have one system that, as you as a pilot come to the checkpoint, you are in uniform, you present your identification, that a security officer there at the checkpoint can either use a smart phone or a laptop to verify that you are in good standing at the time you are checking in there, and then we would proceed with that.

I do want to have several months of success Nation-wide with the pilots before we move on with the rest of the flight crew.

Mr. CRAVAACK. Excellent. I appreciate that.

Will biometric be incorporated in this pilot early-on type of program in order to identify the pilot? Or how do you see it, just a card ID or——

Mr. PISTOLE. We have talked about biometrics, and that might be an end-state we build to. But because of the additional cost and time that is involved in that for everybody, I wanted to do something, initially, recognizing pilots as the most trusted people on the aircraft, regards of what prohibited items they may have.

I think I testified previously, in my last job in the FBI, I worked on the Egypt Air 990 crash off the coast of Rhode Island, Halloween night of 1999—I was stationed in Boston at the time—where we learned later, of course, it was the co-pilot who put the flight down, killed 232 people on board. So no amount of physical screening would have detected what was in his head, and so what if a pilot has a prohibited item? I mean, not being crass, but that is what it comes down to.

So that is where we are going toward. I am very hopeful that we will have something here in the near future.

Mr. CRAVAACK. Yeah, I always found it kind of ironic they were taking my nail clippers when I have a crash axe this big behind me, you know, with a spike and a serrated edge.

But my next question is just kind of a side note, as well. I do have a bill that is presented in identifying our service members that are coming back or on PCS orders that are—the catalyst was, going through the airport, I am seeing a young troop coming back from Afghanistan, still had dirt of Afghanistan still in his boots, and he has his pack as a reservist, and he is coming home. You know, I saw him undo his boots and go through all of the

rigamarole of going through TSA. I do have a bill out there that would expedite this procedure.

Do you see this possibly developing into, like we were talking about, a trusted-passenger type of program, as well?

Mr. PISTOLE. I think members of the military, especially those in uniform and that we can have some positive identification, make sure they are who they purport to be, are a group of people that we would look at in some type of trusted-traveler system. So it is something that we are looking at and trying to assess how do we actually make that happen.

Now, members of the military who are in uniform are supposed to be allowed to keep their boots on, so that is an issue, if that was not the case. It gets back to that standardization issue across the country.

But it is something that we are very much interested in, recognizing that we train them and they are over there protecting our freedoms, and yet we put them through—that being said, also in my last job, I worked on the Major Hasan investigation, and recognize that there are no guarantees, that we are in the risk-mitigation business, not risk-elimination, that any person in a trusted category may break bad, frankly, at some point.

But, as a general rule, if there are things we can do in terms of expediting, that is what we are interested in doing.

Mr. CRAVAACK. Thank you very much, sir, for your testimony.

Mr. Chairman, I yield back.

Mr. ROGERS. I thank the gentleman.

The Chairman now recognizes the Ranking Member, my good friend from Texas, for her opening statement.

Ms. JACKSON LEE. Mr. Chairman, thank you.

Let me express my apologies to my colleagues and the Members here. We were engaged with the very extensive meeting with the President and, as we speak, just finishing that meeting. So I ask the administrator's indulgence and the kindness of the Chairman and my colleagues.

Mr. Pistole, we live in a tough, tough time. I don't believe that you have been before this committee since the miraculous but also instructive taking down of Osama bin Laden. The Chairman knows that, as often as I can comment on the intelligence community, the Navy SEALs, the broad National security team of the President, and President Obama, I do so. It goes without saying that I, likewise, thank the men and women of the Transportation Security Administration and TSOs, who I have joined with as being on the front lines.

We say that because, in the materials that have since been made public, interestingly enough, from the encampment that Osama bin Laden had, it seems that a lot of materials, public materials, focus on transportation. They focus on rail. There is no doubt that there is an attraction to aviation.

As you will recall, after 2009, the Christmas day bomber, the Secretary of Homeland Security made around-the-world trips to begin to talk about the agreements that we have.

I am going to share my thoughts with you very briefly, and then the Chairman is going to call on another Member, and then I will have a line of questioning along the tough climate that we live in.

Thank you, Mr. Chairman.

We have begun the very important process of drafting legislation for the TSA. I welcome our witness today, who has already been welcomed, Administrator Pistole.

TSA's scope of responsibility is broad, and its mission of securing transportation against terrorist attack is critical to the Nation's overall homeland security efforts. I believe that there is a common agreement on this committee between myself and with the leadership of Chairman Rogers. We work together.

Over the past several years, this subcommittee has evaluated cargo security on passenger planes, passenger and baggage screening technology processes, security at foreign repair stations, general aviation, the Registered Traveler program, and the administration of TSA's programs for surface transportation and security.

We understand and support a layered approach to security, whereby if one security protocol fails, there will be others to mitigate the terrorist threat. I remind you, in my opinion, Mr. Pistole, 9/11 was where the overlay did not work. There was not redundancy, and, therefore, we found ourselves in this horrific condition.

As we move forward in this authorization process, we must not forget this basic homeland security tenet: Redundancy, overlay, and "I have your back."

Furthermore, it is important to remember that our last line of defense, the final layer against a terrorist threat is not technology but people. These people are our Federal air marshals, who have been authorized to protect the cockpit and secure the aircraft cabin in emergency. These people are the flight attendants, who, in just the last few months, have subdued several unruly passengers in separate in-flight events and who have consistently asked for required flight attendant training. These are the people we must invest in by authorizing criminal investigative training for FAMs and recurrent advanced self-defense training for flight attendants.

Our pilots', including the Federal Flight Deck Officer, participants are critical. Behind the hardened cockpit doors authorized after the 9/11 attacks, pilots not only are operating the aircraft but providing yet another line of defense. We need to ensure they have the resources in the FFDO program to support their mission.

Outside the aircraft, our people on the front lines are the transportation security officers, who screen 2 million passengers a day. For these TSOs, we need to afford them excellent training and career advancement opportunities that complement the collective bargaining framework.

Administrator Pistole, when you decided and moved quickly to alter the screening techniques and called them "enhanced screening," I went out to my airport, one of the largest in the world and certainly one of the largest in the United States, to stand alongside of the SFD there and watch our TSOs as the public traveled through to be able to ensure, first of all, the confidence of our respect for their process, to ensure that we wanted them to be professional, and also to watch the traveling public accept the fact that we live in a different time. It does not mean that we diminish and aren't concerned about civil liberties and civil rights, about the inspection of elderly and disabled and children, but it does mean that we have to work together.

Speaking of people, Administrator Pistole, I understand from my staff that we have received some of the information I requested on TSA's executive-level diversity, but it may be unbeknownst to you, it was incomplete. We will be working with your office to get the exact type of information we need, and we thank you for the first start that you have made.

Mr. Chairman, I know from my discussion with you that we share the same commitment to securing our Nation's transportation systems. In particular, we have discussed the importance of focusing on securing mass transit and other surface modes of transportation. I thank you again for your commitment to working with this side of the aisle so that we can approach these issues in a comprehensive manner. I certainly hope that, together, we can look closely at my legislation on surface transportation so we can find common ground. We had broad bipartisan support for our TSA authorization bill in the last Congress, and I hope you will look at some of those provisions.

Might I also say, Mr. Chairman, that your concern and interest in K–9s is well-placed, because, as I have traveled, I have noted, from all perspectives, whether it is in the deep bowels of some of our South and Central American friends, looking at the issues of drugs and the overburdensome actions of drug cartels, or whether it is in assisting the traveling public, or whether it is actually bomb detecting, K–9s can be very effective. So I look forward to working with you on that issue, as I hope that we will focus on the needs of surface transportation security and include that issue, along with others, in this year's measure.

I will make just a final point as I close and say that I am looking forward to working with you. I hope also—this is for the whole Department of Homeland Security—that we will unabashedly buy American. I will discuss that further as I proceed in my questions.

But I also ask, Mr. Chairman, unanimous consent that a statement from the National Treasury Employees Union be inserted in the record.

Mr. ROGERS. Without objection.*

Ms. JACKSON LEE. With that, I yield back. Thank you.

Mr. ROGERS. The Chairman now recognizes Mr. Walberg for any additional questions he may have.

Mr. WALBERG. Thank you, Mr. Chairman.

Flowing from the Ranking Member's statements, Mr. Pistole, I would ask, in light of the intelligence discovered in bin Laden's compound, what changes or enhancements does TSA plan to implement in terms of its surface security initiatives?

Mr. PISTOLE. Following the initial triage of documents seized in that raid and the assault, we made some immediate changes, particularly in three areas.

One is the information that we shared with our State and local stakeholders in the rail arena, both the local police but then particularly the Amtrak police. Because the one piece of information from February 2010 was the notation that on the 10th anniversary there be some attack on northeast rail, presumably Amtrak. So that was the first part.

---

*Information was not received at the time of publication.

The second was we increased our random and unpredictable patrols through the VIPR operations, the Visible Intermodal Protection and Response, along with Amtrak and then along with other State and local police, in terms of just trying to be, again, random and unpredictable for anything that may come as a result from the killing of bin Laden. So, is there somebody here in the United States currently who wants to do something to "retaliate"? So that was one of the issues.

Then the third area was to assess the—given the additional intelligence that continues to come out of there—because, you know, the initial triage has been done, and now the deep dives are being done. So I get a daily intelligence brief—in fact, this morning, new, updated information, which I would be glad to provide in a classified setting—as to some more, not specific threat information, but just background on bin Laden's focus on the transportation sector, both the aviation and rail, for the economic impact that it could have and which 9/11 had and other things.

So we are basically rescrubbing from an intelligence assessment to say, do we need to re-baseline where we say the threats are and looking at the traditional equation of what is risk: Threat, vulnerability, and consequence. So, how do we inform our risk judgments based on those threats, the vulnerability of those resources, and then the consequences of a successful attack?

So those are the three actions that we have taken since then.

Mr. WALBERG. From a technology standpoint, what could Congress do further to empower TSA and DHS as a whole to work with the private sector to develop the necessary technologies to ensure our rail and mass transit infrastructure is secure, at least as secure as it can be?

Mr. PISTOLE. Yeah, so I think one of the keys there is, you know, do we set up an airport-type apparatus at rail hubs and transit points? That is a huge lift, I think, so I wouldn't ask for that.

But I think where we can truly benefit, knowing that the three areas that terrorists have identified as possible deterrents, depending on whether it is a suicide bomber or not, but the first two, uniformed officers and K–9s, those are deterrents to any possible terrorist. The third deterrent, CCTV, is only a deterrent for those nonsuicide bombers. So if you are a suicide bomber, as we saw on July 7, 2005 in London, you know, the one terrorist looks right at the camera before he goes down into the Tube and 10 minutes later is dead.

So I think anything that, from a technology standpoint, it is as much—is there additional technology out there? I mean, there are some things that are mechanical—vapor-wake dogs, which there is research being done on that. I am a proponent of the actual dogs because of their effectiveness. But I think it really comes down to that human part, additional officers' training, dogs, and CCTV. So those are the three critical areas that I would see.

Mr. WALBERG. Okay.

Thank you, Mr. Chairman. I yield back.

Mr. ROGERS. I am really glad to hear you mention CCTV. There has not been much talk in this committee about it, but, as we see over in Europe, it is a vital tool in trying to particularly discover what happened when we have an attack.

But I now recognize the Ranking Member for any questions she may have.

Ms. JACKSON LEE. Thank you very much.

I am going to pursue my line of questioning that I followed in laying the premise of the different climate in which we live post the demise of Osama bin Laden. I do want to make it clear that I think America is safer now than it has ever been. It is just that the odds and the life that we are playing with, the general atmosphere in which we are playing at this point, the arena, is far different than 10 or 20 years ago.

So I would like to start first with what improvements you think and what familiarity you have and the work that is being done to secure our foreign repair stations. Because, over the years, we view that as a great vulnerability, and it is something that is not usually high on the radar screen.

Mr. PISTOLE. It is an important point, Congresswoman, in terms of, if we don't have confidence in those foreign repair stations, either in the screening of the personnel, the mechanics who work there, or in their quality control of the products that they are using—all things that industry, obviously, has a keen interest in and regulates, you know, in private industry's sense of the term.

I think we would have to really get into specifics as to which foreign repair station, because of the ones that the TSA has looked at, we have actually found a number to be commensurate with U.S. standards.

That being said, you know, with over 285 or so last points of departure to the United States and a number of repair stations that are either at airports, such as in Europe where many of the repair stations are actually at major airports——

Ms. JACKSON LEE. Correct. My question is how many we have been able to inspect and how many more we have and do we have an at-risk standard.

Mr. PISTOLE. We do——

Ms. JACKSON LEE. That is a big number.

Mr. PISTOLE. It is. I don't have the exact number. But our challenge is to, again, have some level of confidence that what they are doing is not just on the day or the week that we are there inspecting, but that it is happening 365/24/7. That is where we are lacking, frankly. That is one of our gaps. Just based on resources, we can't do that.

So we work with both the country teams and industry in a partnership to say, what are you doing to assess that, and then what can we do to augment that, recognizing that it is one of those areas of vulnerability.

Ms. JACKSON LEE. How do you hold the airlines responsible? What is the oversight there? What is the demand on the airlines?

Mr. PISTOLE. So we have our baseline standards of what is required at any repair station and, of course, working with FAA on their certification of those stations. How that works is, if they are not in compliance, then it is a combination between TSA and FAA to make sure that they are in compliance, and if they are not, then we can take regulatory action, either in terms of a fine or even the ultimate of shutting that repair station down for any work to be done on flights coming to the United States.

Ms. JACKSON LEE. Do you know how many TSA staff, personnel you have on the foreign repair station and what kind of partnership you have with FAA?

Mr. PISTOLE. I have some numbers in my head, but I am not sure. I would like to check on those to make sure I am accurate, so let me get back with on you that.

Ms. JACKSON LEE. I mentioned the difficulties that flight attendants and passengers seemingly had, really it seemed in the days after the demise of Osama bin Laden. Some of those occurrences unfortunately involved individuals who are mentally challenged.

I, frankly, believe that the training for flight attendants should be required. That is not the case now. I would like to know your assessment of that in terms of, again, a changed neighborhood and a changed arena in which we live.

Mr. PISTOLE. Well, I agree, Congresswoman, that additional training would be beneficial, whether it is required—and the question of who pays for it. You know, do the airlines pay for it? Do they provide the time off? Do they provide the travel expenses?

So we have trained—I would have to check the number, but a sizable number of flight crew, flight attendants, in terms of basic defensive techniques and how to engage and work in terms of defusing a situation. So some of that has been done voluntarily.

But you raise a question about, if it is legislated or if it is regulated, then, basically, who pays the cost of that? So that is one of the issues that we have looked at.

Ms. JACKSON LEE. Let me do something very unusual. Let me ask you, Administrator Pistole, to make an assessment. FAMS, as you well know, provides free training. Again, nothing is ever free; there is probably some cost in your budget. But what I would argue is, we didn't do a lot of things around 9/11, and, ultimately, though we don't point to ourselves as the blame, unfortunately a horrific act occurred. In this instance, I think it is worthy of a review. I am certainly interested in legislation.

But I would ask the question, is the cost more to require airlines to be consistent in the training that flight attendants get? Or is it more costly for some person attempting to do harm, with all of the layers and redundancy we have, to make it finally on the airplane and to be able to create a horrific incident where our flight attendants could be ready and prepared to have stopped it—as they did, possibly untrained, with the shoe bomber and as they noticed the Christmas day bomber acting erratic, and quick action was taken. But consistency does not exist.

Would you consider moving internally, while some of us want to rush ahead, which we might just do, but would you—you see my point of the consistency issue.

Mr. PISTOLE. Oh, I do, madam. I think it is a good point. It is a question—again, we do provide the training at no cost. The question is—and if you have airline executives in, that might be a good question for them, in terms of are they willing to support that in terms of having time off. Is it for 4 hours, is it for 2 days? Will they pay the travel expenses to where we do the training and things like that? So those are questions.

But we do that training.

Ms. JACKSON LEE. Well, let me just make an editorial comment. We are paying for pillows, blankets, hot dogs, potato chips, drinks, and baggage. So the mere idea of time off cannot be that excessive for the airlines.

I would commend to you, I would like to hear back from you on this issue.

Mr. Chairman, I am very interested in this, and I think it is valid.

We are getting to go to the floor, and there has been some discussion about collective bargaining rights for the TSOs. Let me commend you for the deliberative and studious way in which you have handled it. I hope everyone appreciates it.

I would appreciate if you would give a very quick summary, and really quick, to say that you obviously made a decision—why don't I just ask the question—after you studied it, that this would not undermine, the way you have structured it, undermine the first-responder security role that TSOs have.

Would you comment on that please, on the issue of collective bargaining?

Mr. PISTOLE. So the issue came down to the authorities granted to the administrator under the Aviation Transportation Security Act of being able to decide what should be subject to collective bargaining. In my judgment, the things that I included, that allowed the security officers to vote on, included those things that I would describe as more administrative in nature—shift bids, uniforms, and things like that, consistency and uniformity in evaluations, as opposed to the actual security screening.

So anything that had a security nexus I said was not subject to collective bargaining. That is obviously the way we are moving forward in this run-off election that is taking place right now.

Ms. JACKSON LEE. You feel comfortable that your men and women in TSA were prepared to be on the front lines and not inhibited by the structure of giving them basic rights that would enhance their confidence and enhance their teamwork through the collective bargaining process.

Mr. PISTOLE. Yes.

Ms. JACKSON LEE. Last, on that issue, if there was a catastrophic incident at one airport that then required a massive moving of some to come in—and we have had it where snowstorms have shut down, and individuals couldn't get to the airport, but you could fly people in—you have that ability, still, to move your personnel around to address the questions of need in this country.

Mr. PISTOLE. With all security officers, except those assigned to the 16 airports under the Security Partnership Program, the SPP. So I don't have that discretion over those individuals.

Ms. JACKSON LEE. Okay.

Let me just add this point about looking and ensuring that, as you buy equipment and uniforms and gadgets and widgets, that, at least under the procurement system that you have and then taking the message back to the Department of Homeland Security, that you will look to products that are manufactured here in the United States.

Mr. PISTOLE. Yes. I understand there has been some discussion and perhaps a bill introduced in that regard by another Member.

So, yeah, obviously, we are interested in following all the laws. As I understand—I got a briefing on the way up—is that we are in full compliance with NAFTA and an amendment to that. So, yeah, we obviously need to do that.

Ms. JACKSON LEE. Mr. Chairman, two last questions.

I think this committee should be aware of the fact, and you should be aware, Mr. Pistole, that there are State legislators and legislatures that have tried to pose legislation—my State, in fact—about the inspection and the AIT. Fortunately, there was a pushback.

I think we are going to have to be particularly attentive to that kind of effort. I really think the outreach, your FSDs, the National outreach in terms of your sensitivity to how you address passengers is very important.

I would like you to comment on three questions put together: That one; and TSA beginning to implement a risk-based approach to passenger screening at checkpoints. Because, again, I am told by some of your leadership that, because airlines are charging for bags, that it has put a whole new burden on your officers and the time frame, which many passengers believe you are slow. I think it is important to acknowledge that there is an extra burden.

But I would be interested in your assessment on the risk-based approach. Then I would be interested in what work you have done—this goes to the Christmas day bomber—on the last-point-of-entry security that I believe is extremely important to you.

If you could. The Chairman has been very indulgent. I will just conclude; you may have to do this one in writing, just to let me know, have there been any EEOC cases filed against TSA and, if so, how many. That may be in writing.

Mr. PISTOLE. I will have to get back in writing on that last point.

Just briefly, in terms of the legislation, we have been engaged with Department of Justice. I am sure you are aware that one of the U.S. attorneys in Texas sent a letter to the Lieutenant Governor and to the legislature outlining some of the legal perils and the supremacy issues involved in that. There have also been some discussions and we have done some briefings that have been helpful, I believe, in terms of providing what the threats are. So that continues, and we watch that closely. We have 3,500 security officers in the State of Texas, and they are all concerned about that, obviously.

In terms of the risk-based——

Ms. JACKSON LEE. I would just say that this may be a creeping activity across various States.

Mr. PISTOLE. Right. There are approximately a dozen States that have some interest in this at various levels that I am aware of.

I have covered in some detail the risk-based security while you were at the White House. I would just summarize by saying, we are very interested in moving forward with all deliberate speed in terms of trying to provide the best possible security by focusing on those that we know the least about as being the highest risk. Those selectees and no-flys, obviously, we know a lot about, and we do a proper, thorough screening with them.

But if we can expedite the screening experience for those that are willing to share information with us or that we already know

a lot about because they have already provided a lot of information, such as in Global Entry or those with Top Secret security clearances or other groups of people, then we are very much interested in that and working deliberately on that.

So there will be more to come on that later this year and——

Ms. JACKSON LEE. On the at-risks?

Mr. PISTOLE. On the?

Ms. JACKSON LEE. More to come on—I didn't hear what you said.

Mr. PISTOLE. On the whole risk-based security——

Ms. JACKSON LEE. Right. All right.

Mr. PISTOLE. The bag fees I touched on earlier, but, yes, we are doing approximately twice as many checked bags now as we did 2, 2½ years ago. So it puts an additional burden and onus on the security officers reviewing each screen and seeing what may be in there as a potential IED component, and so that is a challenge for us. That is what is slowing it down, as opposed to the passenger screening. So that is one aspect we are——

Ms. JACKSON LEE. I think that is important to—I mean, I think in your discussions with airlines, your discussion with the traveling public, you have videos that you put into airports. I told you I would like it to be a little bit more conspicuous. But it is very important in terms of setting the tone for the traveling public.

Mr. PISTOLE. Right. Yeah, you may have heard my public-service messaging in certain airports, encouraging the public to work with us in a partnership, and the better prepared they can be as they travel, the better job we can do and make it a better travel experience for everyone.

On your last point, the last points of departure, we work very closely with both the airport authorities, the civil aviation authorities in those countries, and the industry itself to ensure that their standards on any of the LPDs, as we call them, are to the standards that we have in the United States.

So, in many places, for example, at London Heathrow, Terminal 5, which are the LPDs to the United States, they have additional screening that flights to the rest of the world do not have. So we do work very closely with them.

We are continuing discussions with groups such as ICAO, the International Civil Aviation Organization, IATA, International Air Transit Association, and all industry groups and associations to try to make sure we have a baseline, common standard that enhances security, given the current threat environment.

Ms. JACKSON LEE. Thank you, Mr. Chairman.

Let me thank you for that.

I will put another question on the record, Mr. Pistole, to be answered in writing. That is whether or not you have any specific programs, policies to increase diversity at the executive and non-executive levels at TSA. As you well know, diverse backgrounds are very helpful.

I do want to commend Colonel Testa, who was our FSD at IAH. I understand that she may be detailed here to Washington. That does not make us happy, but it does say what a credible and responsible leader she is. I hope that we have the ability to have her return, if that is at all possible.

To basically thank the overall team that you work with, and that we will continue to work with them.

I think I have submitted this letter into the record. Is this the statement here? Yeah, I think I have asked, and I think the Chairman has already asked unanimous consent for this letter to go in.

So let me yield back, Mr. Chairman. I will look forward to some of the questions that I posed in writing.

Again, Mr. Chairman, I would like to suggest our common agreement on the whole issue of "Buy America," but also this flight attendant training is something I hope we can look at together, and that we can look at this last point of—this last point of departure is a very important issue, in terms of people coming into the United States by aviation travel.

I thank the gentleman for his indulgence.

Mr. ROGERS. Count on it.

We have been called for votes. I don't know what happened; the bells didn't go off. But I just got a note.

But I just wanted to close on one point and kind of get your feedback, and that has to do with the behavior detection officers. How is that going? I understand GAO had a report with some criticisms. Where are you going with that?

Mr. PISTOLE. The GAO did come out with a report that offered some constructive comments in terms of how we can improve. DHS's Science and Technology Directorate looked at that and, actually, has just published a report that, although much of it is sensitive security information, strongly endorses and validates the behavior detection program. I would be glad to get, in a closed setting, into some specific details.

But I received a detailed briefing on it, actually, this morning. It is notable in terms of the success that the behavior detection officers have versus just random samplings, if you will. So it is multiple times more effective than just random. So I am encouraged by that.

That being said, I am interested in upgrading and expanding, in terms of the backgrounds and the capabilities of those behavior detection officers, that will then be wrapped up into a risk-based security program that includes additional behavior detection as part of that.

Mr. ROGERS. Excellent.

Well, listen, I am not going to drag you up here any more often than necessary. You just have one of your staffers come over, and let me and the Ranking Member know what you are going to do. We will do it in a classified manner.

With that, we are going to adjourn this hearing. I want everybody to understand, and you and your staff, that some of the Members who were here may have some written questions. So, in the next 10 days, I would ask you to respond to those in writing, if you get them.

Anything else?

Ms. JACKSON LEE. Mr. Chairman, I thank you very much for, again, the indulgence of some of us who had to come to the hearing late. Thank you very much.

Mr. ROGERS. Great. Thank you.
This hearing is adjourned.
[Whereupon, at 5:13 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN MIKE ROGERS OF ALABAMA FOR JOHN S. PISTOLE

Question 1a. Is the total security approach currently in place at U.S. airports integrated or fragmented? Is there one agency designated with overall responsibility for security at any U.S. airport?

Are the images of approaching vehicles captured by airport security cameras, monitored by TSA in real-time or by another security entity separate from TSA?

Question 1b. Do you think TSA should have access and control of airport CCTV cameras and systems?

Answer. Security at U.S. airports is a collaborative process among several entities. The Transportation Security Administration (TSA) maintains responsibility for screening and ensuring compliance with certain Federal regulations. TSA works with airport authorities at TSA-regulated airports required to adopt and carry out a TSA-approved security program under 49 CFR Part 1542, and collaborates with State, local, and Federal law enforcement agencies on criminal matters. Among other requirements, airports required to have a complete or supporting airport security program must include a description of law enforcement support.

Airports operate and monitor security cameras along with their respective law enforcement and/or security response component as outlined in their airport security programs. The placement, numbers, and types of cameras, as well as the monitoring function (real-time or exception-based), will vary depending on the airport's operational characteristics and available funding. TSA's use of images generally occurs following a security violation or incident, for forensic purposes, and in conducting post-incident reviews and investigations.

While TSA personnel do not directly control the physical operation of Closed Circuit Television (CCTV) cameras, TSA has access to the airport's CCTV cameras and systems. TSA coordinates with airports when it is necessary to review camera footage in support of inspection, investigation, and regulatory duties.

Question 2. Does the current passenger vetting process include any engaged questioning by TSA, the answers to which might suggest suspicious behavior or criminal intent on the part of the passenger? If such intent is suggested but not conclusively established, does the passenger move to another line where secondary screening is effectively in place? If not, why not?

Answer. TSA's Screening of Passengers by Observation Techniques (SPOT) program trains Behavior Detection Officers (BDO) to engage passengers in casual conversation throughout the screening process to observe for behavioral anomalies that may be indicative of potential terrorist or otherwise threatening behavior. If a passenger's observed behavior rises to a pre-determined threshold, the passenger is subjected to additional screening to include a more in-depth conversation element and possible law enforcement notification for resolution.

Question 3. Why is it that U.S. carriers operating abroad with U.S. destinations utilize the enhanced screening approach and yet this approach, while readily available from a private contractor, is not utilized at U.S. airports?

Answer. The security measures referred to are contained in the Transportation Security Administration (TSA) Aircraft Operator Standard Security Program (AOSSP), as the "passenger prescreening security interview." These measures must be conducted by U.S. aircraft operators operating in an overseas environment.

On August 15, 2011, TSA began an enhanced behavior detection proof of concept at Boston Logan International Airport (BOS). TSA Behavior Detection Officers at BOS have undergone additional training and significant on-the-job training in the enhanced screening approach available from a private contractor. BDOs piloting the proof of concept at BOS engage passengers in casual conversation consisting of 3 to 6 brief questions relating to a passenger's trip. More thorough interviewing may occur if concerns arise from the initial BDO engagement.

In addition, the Screening of Passengers by Observation Techniques (SPOT) program operates in many U.S. airports.

Question 4. In which airport(s) are you currently piloting an enhanced passenger vetting security feature based on TSA verbal engagement with the passengers?

Answer. The Transportation Security Administration is conducting a proof of concept that tests an enhanced passenger vetting security feature at Boston-Logan International Airport. If the proof of concept is successful, these enhanced passenger vetting procedures will be piloted at Detroit Metropolitan-Wayne County Airport (DTW). In addition, the Screening of Passengers by Observation Techniques (SPOT) program operates in many U.S. airports.

Question 5. Has TSA successfully implemented a reduced screening requirement for known low-risk passengers such as frequent flyers?

Answer. The Transportation Security Administration (TSA) is undertaking efforts to focus its resources and improve the passenger experience at security checkpoints by applying new risk-based, intelligence-driven screening procedures and enhancing its use of technology. TSA will be conducting a pilot program in the fall to enhance TSA's identity-based, pre-flight screening capabilities and provide lower-risk and known passengers with expedited screening. TSA will test enhancements to TSA's pre-flight, identity-based screening capabilities through a partnership with U.S. Customs and Border Protection (CBP) as well as U.S. air carriers.

TSA will continue to look for ways to enhance its layered security approach through new state-of-the-art technologies, expanded use of existing and proven technologies, better passenger identification techniques, and other developments that will continue to strengthen our screening capabilities.

Question 6. What are the screening protocols for individuals with metal implants, prosthetic devices, or those who need additional care due to special needs travelling in air transportation? Do you believe that any of the protocols should be reformed to better ensure fair treatment of these individuals?

Answer. Persons with disabilities and medical conditions are screened in a manner to ensure they are treated fairly and courteously while mitigating vulnerabilities that are inherent to some devices. The Transportation Security Administration (TSA) works closely with a coalition of over 70 organizations to address the specific concerns associated with medical conditions and disabilities, to include ostomy-related products, prosthetics, and cancer-related treatments. Earlier this year, TSA created a working group comprising of members from TSA's Office of Disability Policy and Outreach and the Training and Procedures divisions of the Office of Security Operations (OSO). This working group regularly discusses screening policy for persons with disabilities and ways to mitigate vulnerabilities while ensuring the best customer service possible. The group also discusses emerging technology and the best ways to screen medical devices. An important outcome of this group was to change the way TSA screens insulin pumps and other medical devices worn on the body. Individuals are no longer required to undergo additional screening of their accessible property or be subjected to an entire pat-down based solely on the presence of one of those medical devices. TSA provides individuals with these medical devices screening equivalent to that other passengers undergo while ensuring the device itself is properly screened.

Specific screening protocols for screening individuals with metal implants, prosthetic devices, or those who need additional care due to access or functional needs are Sensitive Security Information (SSI) and cannot be discussed in this response. However, TSA is available to discuss these screening protocols in a closed setting.

Question 7. Is TSA considering reforming the current standard operating procedures regarding screening children under 12? What are some alternative screening methods other than a modified pat-down that can be used when screening such a child?

Answer. Yes, the Transportation Security Administration (TSA) is working on a risk-based screening model, and has begun testing possible new procedures that may reduce, although not entirely eliminate, the pat-down rate on children. Specific screening protocols are Sensitive Security Information (SSI) and cannot be discussed in this response. However, TSA is available to discuss these screening protocols in a closed setting

Question 8. Are Federal Security Directors and relevant TSA staff required to meet with law enforcement agencies serving the airport? If so, how often are they required to meet? Do they ever exercise or train together?

Answer. There is no specific mandate for Federal Security Directors (FSD) to meet with law enforcement agencies serving the airport. However, FSDs are encouraged to develop and maintain relationships with their law enforcement stakeholders. The frequency of interaction varies among different FSDs and law enforcement authorities.

In support to the FSDs, the Transportation Security Administration (TSA) Assistant Federal Security Director for Law Enforcement (AFSD–LE) is expected to maintain daily contact with the local area law enforcement community. This responsibility has been identified as the primary duty of the AFSD–LEs serving at 82 airports Nation-wide. Typical liaison contacts include the following: The airport police authority; Transportation Security Officers (TSO); TSA regulatory personnel; TSA's Office of Inspections; U.S. Immigration and Customs Enforcement (ICE); Joint Terrorism Task Force; Drug Enforcement Administration (DEA); Federal Bureau of Investigation (FBI); United States Secret Service (USSS); U.S. Customs and Border Protection (CBP); Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF); and other Federal, State, and local agencies whose investigative interests may have a nexus to the transportation systems within TSA's area of responsibility. In this liaison capacity, the AFSD–LE ensures the sharing of critical intelligence information, coordination of investigations, support for security initiatives, and maintaining a proactive law enforcement program to ensure the security of the airport and the traveling public. The Federal Air Marshal Service (FAMS) also assigns Federal Air Marshals (FAM) and Supervisory FAMs to serve as additional airport liaisons between the FAMS, the FSD, and the other agencies listed above.

Question 9. How does TSA determine when private industry should be made aware of certain threats?

Answer. When our intelligence and security partners within Department of Homeland Security (DHS) and the intelligence community (IC) introduce or update threat information, the Transportation Security Administration (TSA) executive leaders of transportation modal subject matter experts and threat intelligence analysts decide immediately whether private industry should also become aware of the information. In many cases DHS and IC liaisons are already working on notification processes out to private industry and coordinate these measures with us. TSA has official relationships with the private industry on global, National, and regional levels, so our capabilities help ensure we are informing all the entities in that customer base.

The immediacy of the threat, the classification of the information and the security clearances of our private industry customers determine the manner in which we share this information. There are multiple technical and organizational solutions available for this type of information sharing. Examples include:

- *National Infrastructure Coordination Center (NICC).*—The NICC serves as an extension of the NOC, providing the mission and capabilities to assess the operational status of the Nation's Critical Infrastructure Key Resources (CIKR), supports information sharing with the ISACs and the owners and operators of critical infrastructure facilities, and facilitates information sharing across and between the individual sectors.
- *Fusion Centers.*—Fusion centers integrate relevant law enforcement and intelligence information and coordinate security measures to reduce risks in their communities. Fusion centers serve as focal points for the receipt and sharing of terrorism-related information. While fusion centers play a vital role in disseminating terrorist information at the State, local, Tribal, and territorial (SLTT) level, there are prominent integrations with CIKR officials as well.
- *Joint Worldwide Intelligence Communications System (JWICS) and Secret Internet Protocol Router Network (SIPRNet).*—JWICS and SIPRNet are systems of secure interconnected computer networks used to transmit classified information in a secure environment.
- *Homeland Secure Data Network (HSDN).*—Functioning as DHS's secure communications infrastructure, HSDN allows Federal and SLTT governments to share timely and actionable classified information.
- *Homeland Security Information Network (HSIN) and HSIN for Critical Sectors (HSIN–CS).*—DHS communicates in real-time to its partners by utilizing HSIN, a highly secure network with a common set of information-sharing functions and tools for various private sector communities with common security interests. System users include Governors, mayors, homeland security advisors, State National Guard offices, emergency operations centers, first responders, public safety departments, and other key homeland security partners. TSA has several portals on HSIN–CS that disseminate information to stakeholders.
- *Non-secure Internet Protocol Router Network (NIPRNet).*—The NIPRNet is used to exchange sensitive but unclassified information between internal users.
- *Intelink.*—A highly secure intranet used by the IC which provides the web environment for protected Top Secret, Secret, and Unclassified networks.
- *National Terrorism Advisory System (NTAS).*—The NTAS communicates information about terrorist threats by providing timely, detailed information to the public, Government agencies, first responders, airports and other transportation hubs, and the private sector. These alerts include a clear statement that there

is an imminent threat or elevated threat. Using available information, the alerts provide a concise summary of the potential threat, information about actions being taken to ensure public safety, and recommended steps that individuals, communities, businesses, and governments can take to help prevent, mitigate, or respond to the threat.

- *National Joint Terrorism Task Force (JTTF).*—Composed on multiple JTTFs sharing information at the regional level. TSA Federal Air Marshals (FAMS) have representatives on selected Federal Bureau of Investigations (FBI) Field Office JTTFs and several of its resident office JTTFs.
- *Interagency Threat Assessment and Coordination Group (ITACG).*—The ITACG consists of Federal intelligence analysts, and State, local, and Tribal first responders, working at the National Counterterrorism Center (NCTC) to enhance the sharing of intelligence with our State, local, Tribal, and private sector partners through established mechanisms within DHS and FBI.
- *Information Sharing and Analysis Centers (ISACs).*—TSA works with transportation industry ISACs on a daily basis to address security issues. Various ISACs have access to and work with the Transportation Security Operational Center (TSOC), and with TSA's modal experts and intelligence personnel. ISAC personnel have access to information and intelligence consistent with security policies.
- *Critical Infrastructure Partnership Advisory Council (CIPAC).*—The CIPAC provides a legal framework for members of the Government Coordinating Council and Sector Coordinating Council to collaborate on a broad spectrum of security activities. This approach aligns with the National Infrastructure Protection Plan (NIPP), the corresponding Transportation Systems Sector Specific Plan (TS–SSP), the Information Sharing Environment Implementation Plan (ISE–IP), and other information sharing guidance. The Sector Coordinating Councils (SCC) plays an important role in providing the private sector perspective on identifying and implementing the information-sharing mechanisms that are most appropriate for their modes of transportation.
- *Working Groups.*—TSA partners with foreign transportation security agencies to share best practices and lessons learned. Examples include working groups within the International Civil Aviation Organization and the International Working Group on Land Transport Security.

TSA will use whichever system or combination of systems that proves most effective in getting the threat information out to private industry.

Question 10. If a TSO is at a checkpoint and fails to detect a threat object during an operational or covert test, what happens to the TSO? Does he remain at the checkpoint? How much discretion does an individual FSD have when deciding how to discipline or when to dismiss a TSO? Do you think there should be more standardized protocols for Federal Security Directors in this area?

Answer. If a Transportation Security Officer (TSO) fails to detect a threat item delivered by the Transportation Security Administration's (TSA) Office of Inspection covert testing team or through the Aviation Screening Assessment Program (ASAP), he/she is removed from screening duties and placed in remedial training. TSA does not discipline TSOs for covert testing or ASAP failures. These tests are conducted to evaluate vulnerabilities and the effectiveness of screening procedures and technology. However, Federal Security Directors have the authority to address TSO performance failures outside the context of covert testing and ASAP.

Question 11. The budget for FAMS has seen an increase each year, yet the FFDO budget has remained relatively flat even though there is wide interest in this program. Have you requested that the FFDO budget be increased?

Answer. Although the administration recognizes the importance of the Federal Flight Deck Officer Program (FFDO) Program, it realizes that funding is limited and has made the difficult decision to distribute scarce available resources elsewhere. The fiscal year 2012 budget request does provide a $313,000 increase to the program's base, which will provide the resources to sustain the FFDO Program at a current services level. The Transportation Security Administration will continue to evaluate its base resource levels to identify efficiencies in order to meet the program's priority requirements, and we will work with the Department and stakeholders to ensure this occurs.

Question 12. In light of the recent revelations of al-Qaeda's interests in attacking our rail infrastructure, what changes or enhancements does TSA have planned in terms of its surface security initiatives?

Answer. In light of the most recent intelligence that al-Qaeda had plans to attack trains or railroad infrastructure, the Transportation Security Administration (TSA) took several actions. In the freight rail mode, TSA immediately communicated with the freight railroad industry and advised them to continue a state of vigilance and

awareness. The effectiveness of this vigilance was demonstrated by the increase in reporting of suspicious incidents detected throughout the railroad industry.

TSA plans to continue conducting assessments of railroad infrastructure, bridges, and tunnels, in particular to assist the railroads with identifying potential vulnerabilities and options to mitigate those vulnerabilities. TSA plans to continue conducting assessments of railroad infrastructure, bridges, and tunnels, in particular to assist the railroads with identifying potential vulnerabilities and options to mitigate those vulnerabilities. TSA's Office of Security Technology, in conjunction with the Department of Homeland Security (DHS) S&T Office of Research and Development, is identifying innovative technologies that can be used in the freight rail environment for intrusion detection and early warning of tampering or disruption of railroad infrastructure. TSA is conducting operational demonstration/system evaluations of integrated, multi-technology intrusion detection systems capable of protecting critical infrastructure components. Examples of the technologies being researched include intrusion sensors using fiber optics, wireless reporting of ground disturbances, advanced infrared, millimeter wave, conventional video, and other technologies to protect rail infrastructure, rails right of ways, tracks, bridges, pipelines, and tunnels.

In the mass transit and passenger rail mode, TSA encouraged the transit and passenger rail agencies to increase the frequency and number of Regional Alliance Including Local, State and Federal Effort (RAILSAFE) operations. This program coordinates the activities of multiple agencies who share in the responsibility of securing the rail system against acts of terrorism. In 2010, the RAILSAFE program expanded beyond the Northeast Corridor to other areas in the United States and to Toronto, Canada, and began establishing partnerships with other international transit and passenger agencies. RAILSAFE partners share intelligence, establish prevention working groups, provide incident response, and participate in coordinated efforts to detect, deter, and prevent terrorist activities. TSA encourages continual RAILSAFE operations on a random basis to practice preparing for different types of security threats. Additionally, TSA will continue issuing Security Awareness messages and conducting Operational Deterrence Programs that include training, public awareness, K–9 units, and Visible Intermodal Prevention and Response Teams. The focus of issuing Security Awareness messages and conducting Operational Deterrence Programs will shift from extended periods of time to shorter periods, such as months or weeks. TSA is also focusing on the protection of mass transit and passenger rail right-of-ways through the development of new technologies. In conjunction with the Transit Policing and Security Peer Advisory Group, TSA has developed recommendations for new protective measures based on most likely threat scenarios that could be implemented as needed.

Utilizing the best available information, TSA will continue to provide guidance to freight rail, mass transit, and passenger rail on possible threats and provide support in developing realistic and implementable measures to reduce vulnerabilities and increase the likelihood of detection and prevention of terrorist acts.

QUESTIONS FROM RANKING MEMBER SHEILA JACKSON LEE OF TEXAS FOR JOHN S. PISTOLE

SURFACE TRANSPORTATION

Question 1. Earlier this year, the Department released new grant guidance impacting the distribution of Transportation Security Grant Program. The new guidance revealed a revised risk formula will be utilized when considering applicants. What was TSA's role in developing the new grant guidance with other Department components and stakeholders? Second, how do you anticipate this new grant guidance will impact mass transit agencies across the United States?

Question 2. With recent cuts aimed at the Transportation Security Grant Program, even though 34 million rail and mass transit passengers travel each day in the United States, surface programs only receive 2% of the TSA security funding. How do you plan to address the significant gap in resources between aviation and surface?

Question 3. In the June 2008 DHS OIG report entitled, "TSA's Administration and Coordination of Mass Transit Security Programs" it says "Many State homeland security and transit security officials said that TSA's risk management approach did not account for differences in the infrastructures and needs of cities and their transit systems" and that "Some stakeholders said they had the impression that grant priorities were being set by political appointees, rather than by subject matter experts with knowledge of the region." In developing the fiscal year 2011 Transit Security Grant Program priorities and evaluating submissions, how will DHS ensure

transparency in the evaluation and selection of projects and avoid discounting the risk to a region due to differences in needs? What is TSA's role in ensuring transparency in the program?

Answer. For fiscal year 2011, the Transit Security Grant Program (TSGP) guidance reflects a revised framework that continues to prioritize operational activities, but is more specific about targeting funding for Nationally-critical transit assets to fully remediate vulnerabilities. The Transportation Security Administration (TSA) worked closely with the Federal Emergency Management Agency (FEMA) in developing the revised framework, which maintains the existing risk formula, but revises how projects are prioritized and reviewed. Through conferences, workshops, regional working group meetings, and conference calls, TSA socialized proposals for changing the fiscal year 2011 process extensively in calendar year 2010 throughout the mass transit stakeholder community, including transit systems, law enforcement agencies, the American Public Transportation Association, and the Sector Coordinating Council. TSA also discussed the revised framework with the Transit Policing and Security Peer Advisory Group, which is comprised of heads of security and/or police chiefs from transit agencies across the Nation. As a result, the final fiscal year 2011 TSGP framework incorporated stakeholder feedback.

The intent of the revised framework is to connect funding to measurable progress in reducing risk, while allowing transit agencies to complete existing projects and provide the foundation for future funding on new initiatives. All agencies that were eligible last year were eligible this year (this eligibility was not affected by changes to eligibility for the Urban Areas Security Initiative program) and all project types that were allowable last year are allowable this year. In that way, all agencies could continue security efforts they started with funding from prior years.

Addressing security of passenger railroads and mass transit agencies requires strong stakeholder partnerships and leveraging of State and local resources in coordination with Federal requirements and support. Various statutes and executive directives require that transportation risk activities be determined and implemented collaboratively in accordance with strategic plans developed with security partners. As a result, addressing security in these surface modes of transportation—as part of the Department of Homeland Security's mission to prevent terrorist acts within the United States, to reduce vulnerability to terrorism, to minimize damage from potential attack and disasters, and to improve system resilience after an incident—requires collaboration from planning through deployment of resources.

Reflecting its collaborative relationship with stakeholders, TSA works to ensure transparency in the grant programs through the development of funding priorities that are presented publically in the annual grant guidance, publishing of review criteria and the scoring methodology also in the grant guidance, and reviewing and explaining the criteria and methodology through workshops and conference calls.

Although FEMA facilitates and hosts the grant review panels, with TSA input and assistance, grant priorities are set by TSA based on extensive input from industry stakeholders, including transit systems, law enforcement agencies, American Public Transportation Association, and the Sector Coordinating Council. Further, TSA utilizes the Transit Policing and Security Peer Advisory Group to ensure regional risk is considered and reflected in the funding priorities.

In order to ensure transparency in the review and selection of projects, the exact scoring methodology and review criteria are included in the fiscal year 2011 TSGP Grant Guidance and Application Kit. Further, this scoring methodology and review criteria, including point ranges, is briefed extensively at regional workshops conducted after release of the grant guidance (seven were held for the fiscal year 2011 TSGP). All of these materials are also made available on TSA's public grants website, so that applicants unable to attend one of the workshops can access the materials.

Question 4. How do you plan to make resources available for testing and development projects—directly impacting surface and mass transportation security—at Pueblo or a similar facility?

Question 5. What are your plans for leveraging the excellent training facilities available at Pueblo? Has there been any discussion of housing training materials and courses there relating to the forthcoming regulations for bus, rail, and transit employees?

Question 6. Last year, the White House released a Surface Transportation Security Assessment that included 20 recommendations. What are your plans for implementing those recommendations and what can Congress do to help you in that endeavor? If possible, please elaborate more than the implementation plan, or if necessary, please work with us to schedule a security briefing to discuss your plans.

Question 7. Secretary Napolitano has made public statements indicating that she wants to place more focus on surface and mass transit security. *(http://*

www.tsa.gov/weekly/13009.shtm) What actions has TSA taken to focus resources within TSA for programs to support mass transit security?

Answer. The Transportation Security Administration (TSA) has maintained a robust and innovative program concerning surface and mass transit security technologies since 2006. Beginning in 2008, through means of an interagency agreement, TSA and the Federal Railroad Administration (FRA) have collaborated on projects related to rail security at the Transportation Technical Center (TTCI), the Department of Transportation rail test facility located near Pueblo, Colorado. TSA is continuing this collaboration with FRA, as well as putting in place a contract directly with TTCI for work efforts unique to TSA's requirements.

There are two courses currently being facilitated at the Pueblo, CO, facility in preparation for the forthcoming regulations and assessments in the Highway and Motor Carrier modes that TSA Transportation Security Inspectors for Surface (TSI–S) will be carrying out in fiscal year 2012. The two courses are the Highway and Motor Carrier Safety Compliance course and the Highway and Motor Carrier Security course. Highway and Motor Carrier Safety Compliance is designed to provide participants with the knowledge and skills to successfully interact with stakeholders in the Highway Motor Carrier (HMC) modes of surface transportation and familiarize them with the equipment used by the HMC industry. Highway and Motor Carrier Security is designed to provide participants with the knowledge and skills to successfully interact with stakeholders in the HMC and Over-the-road Bus (OTRB) modes of surface transportation and provides hands-on training in proper search techniques of HMC and OTRB equipment; the course also trains participants proactively in Highway Motor Carrier Security Action Items.

The Department of Homeland Security (DHS) completed risk-based implementation plans for each of the 20 consensus Surface Transportation Security Priority Assessment recommendations, addressing the potential risks to the surface transportation system and its four subsectors (mass transit and passenger rail, highways and motor carriers, freight rail, and pipelines). These plans focus on policy and process improvements in the general areas of information sharing, Federal agency coordination and grant programs. The timelines to implement the recommendations vary in length; 10 recommendations have been fully implemented and others are scheduled to extend into fiscal year 2014. DHS and its security partners are implementing these recommendations within current staffing and budget constraints and require no additional resources.

In fiscal year 2010, TSA received 15 new surface Visible Intermodal Prevention and Response (VIPR) teams and the fiscal year 2012 President's request seeks 12 additional multi-modal teams. TSA also has established a liaison position between the VIPR group and the mass transit and passenger rail policy and stakeholder outreach group to ensure a closer working relationship and enhanced TSA VIPR team activity in the mass transit and passenger rail environment. This position serves as the TSA Point of Contact for transit-related VIPR issues, and facilitates collaboration with transit security partners to develop risk-based deployment options and determine the VIPR team configurations that will best augment transit security. Also, the partnership between the research and development group and the mass transit and passenger rail policy and stakeholder outreach group has been strengthened through more frequent meetings and status briefs to ensure new developments in technology are not delayed in reaching the prototype stage and field tested at volunteer transit agencies.

GENERAL TSA

Question 8. Who is responsible for airport terminal and perimeter security—TSA or the airport authority? How is this relationship coordinated, and is this issue—coordination between airport operators and TSA on incident response and any other security matters—something that should be addressed in the authorization bill?

Question 9. In your testimony you mention the administration's support for increasing the $2.50 passenger ticket security fee. What operational expenses does this fee cover? What is the budget breakdown between revenue generated from the fee and direct appropriations received from Congress?

Question 10. In the wake of the Moscow Airport attack earlier this year, what steps has TSA taken to improve terminal airport security at U.S. airports which generally have a similar configuration? Are statutory guidelines needed to establish baseline standards for perimeter and terminal security?

Answer. Under the Aviation and Transportation Security Act (ATSA) (Pub. L. 107–71), the Transportation Security Administration (TSA) carries out its responsibility for the screening and inspection of individuals, goods, property, vehicles, and other equipment before entry into a secured area of an airport to ensure effective

levels of security at perimeter access to U.S. airports. TSA requires that each airport operator regulated under 49 CFR Part 1542 carry out a TSA-approved Airport Security Program (ASP) that prevents the unauthorized entry, presence, and movement of individuals and ground vehicles into and within the secured area and airport operations area. Airport operators must also have incident management procedures. Functional measures include ensuring that only those individuals authorized to have unescorted access to the security identification display area (SIDA) are able to gain entry; ensure that an individual is immediately denied entry to a SIDA when that person's access authority for that area is withdrawn and provide a means to differentiate between individuals authorized to have access to an entire SIDA and individuals authorized access to only a particular portion of a SIDA. TSA also approves amendments to an airport's ASP to ensure that alternative security measures still provide an overall level of security equal to or greater than that which would be provided by the measures within the regulation or applicable security directives.

Consistent with ATSA, the Transportation Security Administration September 11 Security Fee is intended to cover the costs for the following aviation security services:

A. Salary, benefits, overtime, retirement and other costs of screening personnel, their supervisors and managers, and Federal law enforcement personnel deployed at airport security screening locations under 49 CFR Part 44901.

B. Training personnel described in (A), and the acquisition, operation, and maintenance of equipment used by such personnel.

C. Performing background investigations of personnel described in (A), (D), (F), and (G).

D. Federal Air Marshals program.

E. Performing civil aviation security research and development under this title.

F. Federal Security Managers under 49 CFR Part 44903.

G. Deploying Federal law enforcement personnel pursuant to 49 CFR Part 44903(h).

H. Security-related capital improvements at airports.

I. Training pilots and flight attendants under 49 CFR Part 44918 and 49 CFR Part 44921.

In fiscal year 2010, Congress appropriated $7.358 billion to TSA (Pub. L. 111–83), of which $2.1 billion is eligible to be offset by the Aviation Security Fee. During fiscal year 2010, TSA generated $2.10 billion in Aviation Security Fee revenue, of which the passenger security fee accounted for $1.81 billion.

In light of the January 24, 2011 attack on Moscow's Domodedovo Airport, TSA has increased security of the public areas of airports by conducting both visible and covert operations. TSA has also developed the Tactical Response Plan (TRP), which details the actions necessary at the field level to support the overall TSA operational response to various scenarios, including an improvised explosive device (IED) attack. Under the TRP, each TSA Federal Security Director and Federal Air Marshal (FAM) Supervisory Air Marshal in Charge (SAC) is required to formulate an Active Shooter Mitigation Plan. This plan describes mechanisms to provide training to employees on how to report emergencies, evacuation procedures, emergency alert systems, and how to coordinate with local law enforcement in the event of an active shooter emergency. All of these measures augment the existing unpredictable security measures already in place at airports.

Question 11. In terms of enhanced pat-down screening, do you still stand by previous statements by TSA that only about 2% of the traveling public is subject to this procedure? Where are you in determining special protocols for children, the elderly, and people with disabilities?

Question 12a. There appear to be more operations between TSA and transit agencies in conducting exercises and testing technology.

Please expound on what efforts TSA is undertaking with respect to securing mass transit.

Question 12b. What has changed in TSA's approach to surface transportation security following the discovery that al-Qaeda has allegedly considered U.S. rail targets?

Question 13. Please describe TSA's efforts to secure pipelines in the United States. Does TSA need statutory authority to further secure the Nation's pipelines?

Answer. Recent data shows that approximately 2.5% of the traveling public is subjected to the Standard Pat Down and .05% of the traveling public is subjected to the Resolution Pat Down during the airport screening process. The Transportation Security Administration (TSA) has developed a conceptual risk-based screening process that includes testing new procedures that may reduce the pat-down rate on children.

Since 2004, TSA has maintained an active, on-going technical and operational assessment and field piloting program of technologies to enhance passenger rail security. TSA has evaluated a range of potentially effective technologies, including those to detect Person Borne Improvised Explosive Devices (PBIED) and Vehicle Borne Improvised Explosive Devices (VBIED), and those used for infrastructure protection. Trace portal technology, and other "checkpoint style" screening technologies were extensively evaluated in 2004 and 2005 by both TSA and the Department of Homeland Security (DHS) Science & Technology (S&T) Directorate. However, resulting assessments determined that "checkpoint style" screening is unsuitable for mass transit rail, or any other high passenger volume mass transit applications.

TSA maintains an on-going program of technical and operational evaluations of commercial-off-the-shelf or non-development item standoff detection technologies. PBIED-related technologies have included millimeter wave, terahertz, and infrared-based systems. VBIED-related technologies have included backscatter portals and vans and high-power X-rays.

Examples of on-going projects include the Resilient Tunnel Project (RTP) and the Under Vehicle Screening System (UVSS). Through the RTP, TSA, in partnership with DHS S&T, is working to create a low-cost solution to limit the flow of water in the event an underwater tunnel is compromised. DHS S&T has assumed funding responsibilities for the RTP. Other partners include the Pacific Northwest National Laboratory, ILC Dover, the Port Authority of New York and New Jersey, and West Virginia University.

UVSS is testing the feasibility and suitability of an under-vehicle surveillance system in the railroad environment. Phase 1 of this project, in partnership with the Port Authority of New York and New Jersey, has been completed, and TSA concluded the technology performed required. Phase 2 of the project, scheduled for July 2011, will test the ability to remotely send images of the undercarriage of a rail car to the Port Authority Trans-Hudson operations center to identify any anomalies. This test is estimated to last approximately 3 weeks.

In light of intelligence that al-Qaeda had plans to attack trains or railroad infrastructure, TSA took several actions. In the freight rail mode, TSA immediately communicated with the freight railroad industry and advised them to continue a state of vigilance and awareness. The effectiveness of this vigilance was demonstrated by the increase in reporting of suspicious incidents detected throughout the railroad industry.

TSA plans to continue conducting assessments of railroad infrastructure, bridges, and tunnels to assist the railroads with identifying potential vulnerabilities and options to mitigate those vulnerabilities. TSA's Office of Security Technology in coordination with DHS's Office of Science and Technology is also assisting with research and development of innovative technologies that can be used in the freight rail environment for intrusion detection and early warning of tampering or disruption of railroad infrastructure.

In the mass transit and passenger rail mode, TSA encouraged the transit and passenger rail agencies to increase the frequency and number of Regional Alliance Including Local, State, and Federal Effort (RAILSAFE) operations. TSA encourages continual RAILSAFE operations on a random basis to practice preparing for different types of security threats. Additionally, TSA will continue issuing Security Awareness messages and conducting Operational Deterrence Programs that include training, public awareness, K–9 units, and Visible Intermodal Prevention and Response Teams. The focus of issuing Security Awareness messages and conducting Operational Deterrence Programs will shift from extended periods of time to shorter periods, such as months or weeks. TSA is also focusing on the protection of a mass transit and passenger rail right-of-ways through the development of new technologies. In conjunction with the Transit Policing and Security Peer Advisory Group, TSA has developed recommendations for new protective measures based on most likely threat scenarios that could be implemented as needed.

Utilizing the best available information, TSA will continue to provide guidance to freight rail, mass transit, and passenger rail on possible threats and provide support in developing realistic and implementable measures to reduce vulnerabilities and increase the likelihood of detection of terrorist acts.

TSA's Pipeline Security Division has issued guidance and implemented risk-based programs to enhance the security preparedness of the Nation's pipelines. TSA has identified the pipeline systems of highest consequence based on the amount of energy transported and evaluated each operator's security program implementation. Additionally, TSA has assessed the level of physical security at critical pipeline facilities. In each case, where appropriate, TSA provided recommendations for security improvements. Further, TSA has established an effective communications network

with the pipeline industry to insure security information is promptly and efficiently provided to stakeholders.

Under the Aviation and Transportation Security Act (Pub. L. 107–71 [November 19, 2001]), and delegated authority from the Secretary of Homeland Security, TSA has broad responsibility and authority for "security in all modes of transportation including security responsibilities over modes of transportation that are exercised by the Department of Transportation." We continue to consider whether additional authority is needed with respect to securing our Nation's pipeline infrastructure.

TSO WORKFORCE

Question 14. There was a GAO report last year that questioned TSA's management of its training program, citing problems with TSO access to computers, as well as TSOs not having the time to conduct training, among other issues. Is TSA addressing the problems identified in its training program? What type of authorization language would help improve TSA's training program?

Question 15. Has TSA updated its training program to include new technologies and procedures, including Advanced Imaging Technology operation and enhanced pat-down screening? Can you assure us that all TSOs are trained on the actual machines they operate?

Question 16. One of my chief concerns has become the need for immediate remedial training when TSO's fail covert tests. It is my understanding that although failures of tests are communicated to Supervisors at checkpoints, information and remedial training does not flow down to the TSO who may have failed the covert test. What steps do you plan to take to ensure that a regimented remedial training program is implemented to ensure that TSOs who fail covert tests are briefed on failure and immediate action is taken to ensure the possibility of human error is mitigated?

Answer. Although we are not aware of a Government Accountability Office (GAO) report which specifically addressed training issues at the Transportation Security Administration (TSA), on October 26, 2010, the Department of Homeland Security (DHS) Office of Inspector General (OIG) released report OIG–11, an audit, of TSA's management of its screening workforce training program. DHS OIG published four recommendations associated with that audit. The recommendations and the action TSA has taken to address them are as follows:

- *OIG Recommendation*.—Documenting processes that are used to determine when and what updates should be made to training materials. *TSA Action*.—TSA is conducting an in-depth training task analysis to be completed in fiscal year 2012 to support a comprehensive review of officer new hire and recurrent training. TSA is also documenting the process it uses to update training materials based on a review of internal and external covert testing results, annual officer certification testing results, intelligence information, as well as updates to operating procedures and deployment of new/upgraded technologies.
- *OIG Recommendation*.—Documenting program efforts underway to formalize an on-the-job instructor training program. *TSA Action*.—Development efforts were underway at the time of the OIG audit, and in June 2011, TSA conducted an operational pilot to determine what efficiencies and improvements in officer effectiveness could be realized with adoption of the program. The review of how this approach may better prepare new officers for their assignments continues, and once completed, a decision will be made on whether a National rollout will begin and whether modifications are necessary before that rollout occurs.
- *OIG Recommendation*.—Documenting a review of training computer allocations. *TSA Action*.—The review is underway, and TSA is taking into account the amount of training that requires computer access, the number of officers at each airport, and the space at airports for setting up computer training rooms.
- *OIG Recommendation*.—Completing a study to determine how to ensure airports provide sufficient time to TSOs to attend and complete scheduled training. *TSA Action*.—TSA is reviewing how it might be able to adopt a customized staffing allocation model that can be used to assess the needs of each airport to account for those locations where travel to and from training locations are required because of off-airport training space, and where airports have a larger inventory of technologies in use and therefore require more time for training on each specific type of equipment.

At this time, TSA does not believe legislation is required to implement any of the recommendations made by DHS OIG.

TSA continually updates its training programs to include new technologies and procedures, including operation of Advanced Imaging Technology and the current pat-down screening process. TSA documents all technical training completed by its officers, and each officer is trained on each type of screening technology that they

are assigned to operate. Training is coordinated to ensure officers are trained on machines manufactured by the specific manufacturers of the equipment used at their assigned airports.

Remedial training for Transportation Security Officers (TSOs) who fail covert tests remains a requirement throughout TSA. Upon such a failure, the TSO is immediately removed from performing the failed security function and may not return to duty to perform that function until he/she has received the necessary remedial training and the training has been documented.

TSA OMBUDSMAN

Question 17a. We have been told that the TSA Ombudsman lacks the independence and authority to get personnel issues resolved. As a result, employees often avoid the Ombudsman and withhold their complaints for fear of retaliation.

To give this office the independence and weight it needs to resolve personnel problems, do you agree that the Ombudsman should have its own office in TSA that reports directly to the Administrator?

Question 17b. Would you support a provision like this in the authorization bill?

Question 18. What will the TSA Ombudsman's role be under the new collective bargaining framework?

Answer. The Transportation Security Administration (TSA) Ombudsman reports to the Administrator through the Office of Special Counselor (OSC), headed by the Special Counselor. In accordance with the Transportation Security Administration's (TSA) Management Directive 100.0.1, *OSC Roles and Responsibilities,* one of the responsibilities of the Special Counselor is serving as the principal advisor to the TSA Assistant Secretary and senior leadership on significant issues and concerns brought to the attention of the TSA Ombudsman from employees, stakeholders, and the public, and through proactive engagement. OSC also oversees the Office of Civil Rights and Liberties (OCRL), giving the Special Counselor a unique, expansive view of the TSA workplace through the informal and formal issue resolution lenses provided by the TSA Ombudsman and the OCRL.

The details of the collective bargaining framework are still being developed. In the TSA Administrator's February, 2011 determination regarding Transportation Security Officers and Collective Bargaining, it concluded TSA would develop a unitary dispute resolution system that included both interest-based and neutral, third-party rights-based options, and envisioned that such a system would permit the existence of a confidential, neutral, informal issue resolution resource such as the TSA Ombudsman. In that framework, the TSA Ombudsman will continue to perform its role of providing confidential, neutral, informal workplace problem resolution assistance to all TSA employees.

TSA AND TECHNOLOGY

Question 19. Administrator Pistole, many of the existing explosive detection system (EDS) machines are reaching the end of their useful life. As one of the first new aviation security technologies deployed after September 11, 2001 many of the EDS machines have been in constant service for nearly 10 years. Will you please provide a detailed plan for the acquisition of new machines to replace the aging EDS machines now in place?

Question 20a. I am increasingly concerned that TSA is taking a stagnant approach to the utilization of innovative technologies in its efforts to achieve 100% screening of air cargo on passenger planes. I have heard from some companies that TSA is overly-reliant on incumbent companies and not testing and approving innovative technologies from other companies that might help us better secure air cargo.

What efforts is TSA taking to ensure that emerging technologies, especially from small businesses, are being approved and used?

Question 20b. When will it next review potential air cargo screening technologies?

Question 20c. Will you consider entering into more pilot programs with innovative non-incumbent companies to test security technologies in an operational setting?

Question 21. CQ noted that TSA is lagging in its efforts to utilize non-contact trace detection for explosives in cargo pallets. The article discussed some efforts undertaken by the Science & Technology Directorate on this front but did not mention whether TSA has actively engaged with companies already operating in this space to come up with standards and requirements for non-contact trace detection. How is TSA preparing to engage in the efforts underway at S&T?

Answer. While continuing to ensure 100% checked baggage screening, the Transportation Security Administration (TSA) will be shifting its focus from completion of optimal airport systems to the replacement of an aging Explosives Detection Systems (EDS) fleet of equipment. EDS equipment is estimated to have a useful life

of 10 years and it is projected that approximately half of the EDS fleet will have reached the end of its useful life by 2013, with up to two-thirds of the fleet requiring replacement within 5 years. TSA is currently working to finalize a Recapitalization and Optimization strategic plan, which will prioritize airports based upon a combination of age and maintenance data. To support this effort, TSA has requested an update to the authorization language regarding the Aviation Security Capital Fund to authorize the purchase and installation of EDS equipment.

TSA and the Department of Homeland Security's Science and Technology Directorate (DHS S&T) continuously explore both the commercial marketplace and technology development arenas to find innovative technologies that might assist in better screening of air cargo. In addition, TSA maintains means to quickly assess promising, technically mature innovations.

TSA and DHS S&T also have several means in place for small businesses to propose emerging technologies. TSA maintains a Broad Agency Announcement (BAA) encouraging submission of new technologies, while also maintaining an on-going BAA specifically for air cargo technology qualification. In accordance with the existing TSA air cargo BAA, TSA intends to offer at least one qualification opportunity for products in each of the major technological groups during fiscal year 2011 and fiscal year 2012. Through this process, businesses of all sizes have equal opportunities for qualification, including several small technology vendors whose products have been approved.

During fiscal year 2011 and fiscal year 2012, TSA intends to offer at least one qualification opportunity for products in each of the major technological groups. Solicitations for explosives trace detection and X-ray technologies were recently conducted. TSA and DHS S&T have several means in place for businesses to propose emerging technologies which provides for review of inputs by technical experts. If a proposal is deemed to have potential for being effective and suitable enough to meet requirements for use in the field, TSA considers the best means of further evaluation. There is full and continuous collaboration between TSA and DHS S&T on all air cargo technology initiatives. It should be noted that threat characterizations and resulting standards and requirements are based on the actual threats, not technology modes. TSA explores effectiveness of all technology modes and qualifies those that are proven to be successful in detecting threats.

TWIC

Question 22. Over the last several years, this committee has spent significant amounts of time conducting oversight of TSA identity management and security program—the Transportation Worker Identity Credential. As we all know, this program has had significant challenges over its short life—the latest of which is TSA's inability to conclude the TWIC reader pilot program and deliver the Congressionally-mandated pilot report. TSA's delays have caused Coast Guard to delay issuance of the final TWIC reader rule. So, we have these very expensive biometric identity cards, which are used as simple flash passes—and clearly, this isn't the intent of the program.

My question is this—when will TSA provide TWIC reader pilot program results to Members of Congress so that readers can be deployed at our Nation's ports, and when will we see the benefits of this program?

Answer. The Transportation Worker Identification Credential (TWIC) reader pilot concluded on May 31, 2011. A draft of the TWIC Reader Pilot final report is currently under Department review. The Coast Guard intends to publish the Notice of Proposed Rulemaking (NPRM) after the Advanced Notice of Proposed Rulemaking (ANPRM) public comments are analyzed and results from the TWIC pilot program are available. The Coast Guard plans to have a full 90-day comment period for the NPRM and have public meetings at various locations across the country. As the Coast Guard evaluates the economic and operational impact on the maritime industry, they will continue to seek input and recommendations to develop and propose regulations requiring industry compliance.

Initial delays in the pilot program were encountered as the Transportation Security Administration (TSA) led a joint effort by several Federal agencies, card and reader industry experts, and maritime stakeholders to develop a specification enabling readers to conduct a biometric match under the harsh conditions found at maritime facilities. Later the field phase of the pilot was delayed due to the voluntary nature of participation in the pilot. This limited the Government's ability to influence the pace at which participants completed site plans, obtained authorizations to expend pilot funds from the Federal Emergency Management Agency (FEMA), and award reader installation contracts. Pilot participants also encountered delays due to technical system installation or parts availability issues. Finally,

the recent economic climate and competitive concerns created significant delays in commencing the pilot at a number of the larger pilot participant facilities. Work force reductions and layoffs caused some facility operators to postpone their participation until shipping volumes increased following the economic downturn. Competitive concerns with non-pilot facilities caused reluctance among some pilot participants to disturb their operations to the extent needed to register the TWICs of thousands of workers and truckers into their access control systems. All of these challenges have now been overcome, all data has been acquired and analyzed, and a final draft of the pilot report completed.

Today, even before the Coast Guard finishes its rulemaking, there are already benefits to the TWIC program, and ports are more secure. Many facilities have already started using readers either installed during the pilot or acquired independently to ensure workers have valid TWICs. Some facilities are fully using the card's capabilities by using biometric matching to verify identity; the facilities choosing to use readers are doing so voluntarily in advance of the reader rule. Some facilities have confirmed cost savings afforded by avoiding the cost of providing facility badges and automating access control. The security director at a major petroleum refinery in Louisiana reported savings of $700,000 per year due to TWIC. The savings result from eliminating costly employee background checks, using TWICs to replace facility badges, and automation of the access process. The Coast Guard also uses more than 200 portable readers to check TWICs during routine facility inspections.

TWIC has already standardized the security threat assessment (STA) conducted on workers, and providing one standardized biometric credential, removing the need to have security personnel discern the authenticity of multiple identity documents. Prior to the implementation of TWIC, the identity document requirements for access to secure areas of ports and vessels were dependent on each facility's Facility Security Plan. Facilities often accepted a number of documents such as a driver's license, passport, State ID, port/facility specific security card, or a Merchant Mariner's Document (also known as a "Z-card" and now known as the Merchant Mariner Credential or "MMC"). Without uniform credential issuance processes, most facilities were unable to positively authenticate the identity of an individual or determine the authenticity of the identity documents presented. There also were no universal methods for determining if a once-valid credential holder were no longer eligible for access privileges, or to effectively revoke an individual's access permissions or credentials.

Truckers have specifically benefited from the TWIC as the one common credential needed for access to regulated facilities. Prior to TWIC some truckers had to obtain, and often pay for, background checks and badges for multiple ports and facilities.

ADVANCED IMAGING TECHNOLOGY (AIT)

Question 23a. There are several legislative measures that have been introduced concerning AIT.

What is your position on prohibiting AIT use until the National Academy of Science has conducted a study of AIT safety as related to radiation exposure?

Question 23b. What is your position on limiting AIT use until the Automated Targeting Recognition (stick figure) software is in place?

Question 24. To what extent would AIT have detected the hidden explosives used in the Christmas day attempted bombing of Flight 253?

Question 25. To what extent has TSA surveyed passengers' willingness to be screened by AIT and addressed public concerns related to privacy and health risks? TSOs?

Question 26a. Since TSA is now planning to deploy about 10 new technologies to passenger checkpoints, how will it ensure that these different technologies are successfully integrated?

Has TSA updated its passenger checkpoint program strategy to reflect the increased use of AIT?

Question 27. Could you provide the committee with a copy of the updated AIT deployment strategy?

Answer. The Transportation Security Administration (TSA) commissioned the U.S. Army Health Public Command to perform radiation safety surveys of currently deployed general-use backscatter X-ray Advanced Imaging Technology (AIT) systems and a radiation dosimetry study to exam the radiation doses to individuals undergoing screening and to system operators. The surveys and study validated that doses to individuals undergoing screening are well below the radiation dose limits of the American National Standards Institute/Health Physics Society (ANSI/HPS) N43.17–2009. *Radiation Safety for Personnel Security Screening Systems Using X-*

Ray or Gamma Radiation, a standard that applies to systems used to expose people to X-rays for the purpose of security screening. Potential doses to AIT operators were found to be extremely small. At the maximum possible throughput, the doses to operators are still below the public dose limits. The American National Standards Institute (ANSI)—Accredited Standards Committee N43, *Equipment for Non-Medical Radiation Applications,* administered by the Health Physics Society (HPS), published the current version of the American National consensus radiation safety standard for X-ray people screening products in 2009. ANSI/HPS N43.17–2009 *Radiation Safety for Personnel Security Screening Systems Using X-Ray or Gamma Radiation* sets limits on dose to an individual being screened; sets limits on dose to bystanders, operators, and other employees; requires a variety of safety features; and establishes operational requirements for organizations using these products. It was written, reviewed, and approved by a consensus group that included Government regulators, product manufacturers, and product users.

AIT addresses the significant security threat posed by non-metallic explosives. Automated Target Recognition (ATR) is an important improvement that addresses privacy concerns among some members of the public. TSA is confident in the privacy protections offered by its existing operational protocols and does not support limiting AIT use during the transition to ATR-equipped AIT. TSA is preparing for deployment of ATR software to all millimeter wave AIT units. The AIT backscatter technology units do not yet have an approved ATR software update.

AIT units address screening for small threat items and non-metallic explosive devices and allow Transportation Security Officers to screen passengers safely and effectively for both metallic and non-metallic threats, including weapons and explosives. After analyzing the latest intelligence and studying available technologies and other processes, TSA determined that AIT is the most effective method to detect threat items concealed on passengers, such as the non-metallic explosives used by Umar Farouk Abdulmutallab in the Christmas day attempted bombing of Flight 253.

Since TSA began piloting its use of AIT units in 2007, TSA has been forthcoming with the traveling public about the technology, including the strong privacy protections in place. To that end, TSA has conducted dozens of press conferences in various locations reaching thousands of passengers to inform the traveling public about the importance of the technology and to advise them that the technology is an optional screening method. In addition, multiple signs informing passengers about the technology, including sample images, are provided in plain sight at airport security checkpoints, in front of the machine, and on the machine itself.

TSA seeks input from the traveling public in a variety of ways via a contact center, feedback at airports and through the TSA website. Polling by CBS, Gallup, Trip Advisor, Travel Leader, and the Wall Street Journal demonstrate strong public support and understanding for the need for the technology:

CBS poll: 81% of passengers support the use of imaging technology.
Gallup poll: 78% of air travelers approve of U.S. airports' using advanced imaging technology on airline passengers.
Wall Street Journal poll: 73.9% of travelers said they would be willing to undergo a body scan before getting on a plane.

TSA also had extensive internal communications regarding AIT technology:

- Developed and launched an intranet (iShare) page dedicated to AIT and AIT safety.
- Used ad space ("Flashbox" images) on the intranet homepage to highlight updates made to the AIT page.
- Posted content to the Employee Communications Committee (ECC) intranet (iShare) site—a site with 300 members across the country including customer service managers, stakeholder managers, AFSDs, and others—for local distribution of HQ-produced AIT-safety products.
- Collaborated with the Office of Security Operations (OSO) Communications (Comms) team to push content through OSO channels directly to the coordination centers, Federal Security Directors (FSDs), and others at the airports.
- Developed, posted, and/or published the following products about AIT and AIT safety:
  - Wrote and posted AIT Facts You Can Use—concise list of bullets with the most pertinent AIT facts, including facts about safety (distributed through iShare, OSO Comms, ECC).
  - Wrote and published multiple internal stories about AIT safety on the agency-wide news blog housed on the intranet (iShare).
  - Linked to AIT-safety reports (linked from AIT iShare page).

- Linked to news reports about AIT safety (linked from AIT iShare page).
- Posted multiple videos about AIT and AIT safety.
- Produced AIT and AIT safety content for the National shift brief (distributed through OSO Comms).
- Wrote FSD talkers—talking points that FSDs could use when talking to stakeholders and staff (distributed through OSO Comms).

The TSA Office of Occupational Safety, Health, and Environment prepared and published a Radiation Safety monthly briefing package that included AIT safety. Safety Week 2011 included the topic "Radiation Safety at TSA" and presented AIT safety. Certified Health Physicists from the U.S. Army Public Health Command continue to perform independent radiation safety surveys of general-use backscatter X-ray AITs. Part of the survey process includes question-and-answer sessions with employees who operate and work near the systems.

TSA employs an agency-wide data management system called the Security Technology Integrated Program (STIP) to ensure that equipment is successfully integrated. STIP provides a centralized focal point connecting passenger and baggage screening security technologies to one network, addressing current data, threat response and equipment challenges. The goal of STIP is to remotely manage Transportation Security Equipment (TSE) threat detection capabilities, which enhances TSA's ability to respond to new and emerging threats. STIP will also enable TSA to remotely monitor, diagnose, troubleshoot, and manage TSEs, allowing TSA to address equipment issues and reduce the need for on-site visits.

The TSA has incorporated AIT equipment and its increased usage into the passenger checkpoint program strategy. This strategy is in the final review/approval phase.

The AIT deployment strategy is sensitive security information (SSI). TSA is willing to separately provide a SSI briefing and a copy of the document to the committee.

AIR CARGO

Question 27. In your opinion, is industry experiencing any supply dislocations due to the 100% screening mandate for cargo on passenger aircraft?

Question 28. How are you ensuring or verifying that the private sector is properly screening the cargo within its jurisdiction?

Question 29. Simply put, what are the biggest challenges to implementing 100% screening of inbound cargo and how can TSA expedite reaching 100% screening for international inbound cargo on passenger aircraft?

Question 30a. Foreign air carriers have said that they can be helpful in working with their own governments on harmonization efforts for cargo screening.

Does TSA plan to work with foreign carriers to help establish reciprocal cargo screening agreements?

Question 30b. Does TSA need statutory authority for this?

Answer. There has been no reported disruption to the air cargo supply chain as a result of the 100% screening mandate implemented on August 1, 2010, for cargo transported on passenger aircraft originating from domestic airports. The Transportation Security Administration's (TSA) comprehensive air cargo screening strategy has successfully distributed the burden of screening cargo across the supply chain; most effectively through the implementation of the TSA Certified Cargo Screening Program (CCSP). Under the CCSP, TSA certifies cargo screening facilities located throughout the United States to screen cargo prior to providing it to airlines for shipment on passenger flights. Participation in the program is voluntary and designed to enable vetted, validated, and certified supply chain facilities to comply with the 100 percent screening requirement. CCSP is a practical, supply chain solution, which provides security while ensuring the flow of commerce. Cargo is screened at the most efficient and effective point. It is done before individual pieces of cargo are consolidated for shipment. Up to and concurrent with the release of the 100% screening deadline, Certified Cargo Screening Facilities (CCSF) have emerged proportionately in geographic regions in response to demand in major air cargo gateways; thus avoiding any potential supply dislocations. The program allows for the use of multiple screening methodologies and has been adapted as necessary to fit each individual situation rather than restricting entities to a single universal solution. Because no single technology is appropriate for every screening scenario, TSA has approved a suite of technologies and associated screening protocols from which screening entities may choose on the basis of their unique requirements and commodities. This current suite of technologies include various X-ray systems, explosive trace detection (ETD) technology, explosive detection (EDS) systems, and electronic metal detection (EMD) systems, as well as physical screening. TSA continues to

identify and evaluate various technologies that can efficiently and effectively screen different types of commodities and configurations. The percentage of cargo screened by CCSP participants indicates that screening consistently occurs throughout the air cargo supply chain without undue burden on any one entity (CCSFs account for approximately 50% of total screening).

TSA is actively conducting inspections and testing screening protocols to ensure that CCSFs and aircraft operators are properly screening 100% of cargo transported on passenger aircraft. These inspections are carried out on a continuous basis.

TSA has established close links with the foreign air carrier community through on-going direct communications via TSA's International Industry Representatives (IIR). IIRs serve as liaisons between TSA and foreign air carriers. TSA also interfaces with the foreign air carrier community through various air carrier associations and related forums.

TSA understands that foreign air carriers play a key role in advocating harmonization of air cargo security requirements between countries. However, TSA believes that global harmonization of cargo security requirements, where and when appropriate, should be handled through government-to-government channels as well as through relevant regional and international organizations, that are responsible for international civil aviation security and that establish the regulatory requirements for air cargo security. Specifically, TSA is currently engaged with a number of countries seeking recognition of National Cargo Security Programs whereby TSA recognizes a foreign government's cargo security programs. To effectuate bilateral and multilateral partnerships and related initiatives in the air cargo security realm, TSA uses already established means of communication, such as its network of Transportation Security Administration Representatives (TSARs) located in key locations throughout the world and through participation in regional and international working groups and related forums. Working through the TSARs, TSA has established close working relationships with foreign government and other international partners, through which we can jointly work on these critical security issues.

In addition to direct relations with foreign air carriers through the IIRs, TSA will continue to leverage established relationships with foreign air carrier associations and forums (for example: the International Air Transport Association, the Air Transport Association, and the Association of European Airlines, and the Association of Asia Pacific Airlines) to advocate harmonization of cargo security requirements on a global scale, as appropriate.

TSA does not believe that statutory authority is needed at this time.

STAKEHOLDER INPUT

Question 31. It has been brought to my attention that the charter of the Aviation Security Advisory Committee (also known as ASAC) has apparently lapsed (again) in April 2010. One of the primary functions of the advisory committee was to facilitate stakeholder input across TSA security policies. What is TSA doing to ensure consultation with stakeholders on security policies, and will the ASAC be re-chartered this year?

Answer. During review of the Department's advisory committees to ensure they are effectively used and an efficient expenditure of resources by the participants, charter renewal actions were placed on hold and the Aviation Security Advisory Committee (ASAC) subsequently expired on April 3, 2010. A new ASAC Charter was approved in May 2011, and the Department of Homeland Security is now in the process of appointing members. The Transportation Security Administration (TSA) anticipates holding a committee meeting early this fall. TSA has always engaged stakeholders, and will continue to do so, through regular outreach and coordination including, but not limited to: Sharing best security practices, including stakeholders in security planning activities, participating in the Critical Infrastructure Partnership Advisory Council (CIPAC), web boards, conference calls, and email alerts.

REPAIR STATIONS

Question 32. How will TSA assess air carrier security programs at foreign repair stations? What roles or responsibilities will be required of air carriers in terms of their own oversight of repair stations where they outsource repair and maintenance work?

Question 33. What statutory authority does TSA need in terms of working with foreign governments to conduct security assessments at repair stations?

Question 34. Will there be harmonization agreements with certain governments where TSA would allow a foreign government's security oversight program to satisfy TSA requirements?

Question 35a. The Notice of Proposed Rulemaking for the aviation repair station security program lacked specificity on staffing requirements to effectively oversee the repair station security inspection program.

Will TSA conduct a staffing study to determine requirements for effectively overseeing a repair station security program?

Question 35b. Some stakeholders informed the committee that they have not been consulted on the repair station rulemaking in several years.

Will TSA reach out to stakeholders for input on how to implement an effective repair station security program?

Question 35c. How will TSA control the dissemination of sensitive security information in its oversight of repair stations, particularly those in foreign countries?

Answer. The Vision 100—Century of Aviation Reauthorization Act, Pub. L. 108–176, codified at 49 U.S.C. § 44924, authorizes TSA to develop and issue security regulations to improve the security of the Federal Aviation Administration (FAA) part 145 certificated repair stations located in and outside the United States. The Transportation Security Administration (TSA) has established procedures for conducting assessments outside the United States through its Foreign Airport and Foreign Air Carrier Assessment Programs and intends to use those same procedures when conducting inspections of FAA certificated repair stations located outside the United States. These established procedures require coordination with the U.S. Department of State and the appropriate foreign government authorities. TSA has discussed and will continue to discuss current and proposed security requirements with its international partners through existing bilateral and multilateral mechanisms in order to enhance the compatibility of security regulations and standards, including the possibility of developing protocols for reciprocity and mutual recognition of repair station security regulations.

TSA has reviewed staffing requirements for the repair station security inspection program. TSA continues to evaluate the resource needs to implement, carry out, and enforce the proposed regulations. Any staffing and resource requests will be transmitted as part of the President's budget.

Throughout the rulemaking process, TSA has engaged the Repair Station owners/operators and associations through meetings and site visits, both foreign and domestic. These visits provided valuable insight into the facilities and existing security procedures already in practice. The proposed regulations were published for public comment in the *Federal Register* and TSA received many comments from repair station owners and operators. TSA has conducted numerous meetings with representatives from major repair station associations, and representatives from active repair station owners/operators, wherein they were given the opportunity to review and provide feedback on the draft Aircraft Repair Station Security Program (ARSSP). Meetings were held in the United States; Portugal; Ireland; Singapore; Germany; and Switzerland. TSA is continuing these outreach effort, including a visit to Thailand on August 23, 2011.

Additional reviews will be planned as necessary. After the rule is published, TSA will leverage headquarters and field inspector resources to conduct significant outreach to all affected repair station operators to ensure they understand, and are able to comply with, the new regulations.

The only sensitive security information (SSI) that TSA will initially generate in support of this rule is the ARSSP. This document will only be provided to foreign and domestic repair stations that will be required to implement a security program. TSA will follow all appropriate markings, protections, and release protocols required by 49 CFR Part 1520 for each release of the document.

GENERAL AVIATION

Question 36. H.R. 2200, the TSA Authorization bill passed by the House last Congress established a grant program for general aviation airport operators for security improvements. Do you think this is something that is needed in the general aviation community?

Question 37. What is the status of the final rulemaking for general aviation security programs and what can you tell us about how it will differ from the poorly received proposed rule issued in 2009?

Question 38a. What steps, if any, has TSA taken to identify and prioritize the need for security enhancements at general aviation airports?

Question 38b. What is the estimated cost of the improvements needed to comply with the proposed regulations?

Answer. The Transportation Security Administration (TSA) will work with the Department of Homeland Security and the White House to assess the feasibility of developing a grant program.

In 2008, TSA published the Large Aircraft Security Program Notice of Proposed Rulemaking (NPRM), proposing rules for U.S. air carriers and GA operators operating aircraft with a maximum takeoff weight of more than 12,500 pounds. In the NPRM, TSA noted the possibility that large turbine-powered GA airplanes are capable of causing significant damage if used in an attack. The 4-month comment period provided in the NPRM was extended another 60 days to obtain additional comment from the general aviation community. During the original formal comment period, TSA conducted five public meetings throughout the country to facilitate feedback by the general aviation community. The comments on the proposals in the NPRM were generally critical of the approach in the NPRM, and repeatedly noted that GA operations differ from air carrier operations. Unlike air carriers, GA operators do not offer transportation to the public for compensation or hire and, in general, TSA has not required GA aircraft operators to adopt security programs. The comments obtained pursuant to TSA's outreach provided additional detailed insight into GA operations and possible alternative security solutions for such operations from those proposed in the NPRM.

Based on careful review of all comments, TSA is drafting a Supplemental Notice of Proposed Rulemaking (SNPRM) that will include proposals tailored to GA operations, while maintaining an effective level of security. The draft SNPRM is undergoing internal Government review and certain provisions could change as a result of that process. After that review is complete, the SNPRM will be published in the *Federal Register* for public comment.

TSA has conducted an airport vulnerability survey to identify the overall security posture at certain GA airports across the United States. The survey was distributed to approximately 3,000 airports that met certain criteria that TSA, in collaboration with industry, identified as the airports that both groups are most concerned about. These were public-use airports with high numbers of GA operations; the ability to accommodate larger aircraft; and in close proximity to densely populated areas, highly used airspace, or in close proximity to sensitive areas or airspace. The results of the survey were analyzed to discover the general strengths and weaknesses at GA airports, as well as to identify and prioritize the security measures that airports might implement if funding were available.

As part of the GA airport vulnerability assessment, certain security measures were identified with their associated costs. The security measures that would be appropriate to implement can vary widely depending on an airport's characteristics and what is already in place. Thus, many of the associated costs also vary widely depending on the size and characteristics of the airport at which they would be implemented. This wide variance in airport characteristics and levels of security prevent a more specific cost estimate. TSA's security focus regarding general aviation is centered around securing aircraft so they cannot be used to do harm and the agency is not currently proposing any regulations for GA airports.

SECURE FLIGHT

Question 39a. We have been told that Secure Flight would generally fix the problem of innocent passengers being mistakenly matched to the No-Fly or Selectee lists, due to a similar name.

Is this situation improving now that Secure Flight is fully operational?

Question 39b. Are you keeping data on passengers requesting redress?

Answer. Yes, Secure Flight has reduced the number of passengers mistakenly matched to the No Fly or Selectee Lists. TSA requires aircraft operators to collect each passenger's full name, date of birth, gender, and Redress Number if available. The use of this data in conducting watch list matching significantly decreases the likelihood of passenger misidentification. Additionally, in May 2009, GAO certified that the Secure Flight system generally met the condition that the system does not produce a large number of passengers being mistakenly matched to the watch list, as outlined in the 2005 Department of Homeland Security (DHS) Act. The Secure Flight program continues to succeed in reducing instances of passenger misidentification.

DHS Traveler Redress Inquiry Program (DHS TRIP) maintains travel data submitted by travelers through the redress inquiry process in accordance with the Privacy Impact Assessment for DHS TRIP. DHS TRIP has received approximately 135,286 redress requests from the public since its launch on February 20, 2007. The results of the redress process are directly integrated into Secure Flight through the Redress Number to prevent the reoccurrence of known passenger misidentifications.

IN-LINE BAGGAGE

Question 40. Some airports have not been reimbursed for terminal modifications made to install checked baggage explosives detection systems because they made expenditures before a reimbursement program was established by TSA, and now these airports are at the bottom of the list for receiving reimbursement. H.R. 2200 directed TSA to establish a claims process for these airports. Please comment on this.

Answer. To provide more effective security solutions, the Transportation Security Administration (TSA) takes a risk-based approach to investing in security programs at airports without optimized baggage screening systems. The *Implementing Recommendations of the 9/11 Commission Act of 2007* (Pub. L. 110–53, Section 1406) requires TSA to establish a prioritization schedule for airport security projects based on risk. In addition, TSA focuses on compliance requirements—such as replacing equipment in the field that has reached the end of its life-cycle—to minimize operational impacts. Due to the number of airports that are awaiting the replacement of sub-optimal baggage screening systems, and other competing program priorities, TSA has been unable to address reimbursement requests. Any reimbursement of previous efforts outside a formal agreement comes at the cost of advancing current or future security measures.

INDUSTRY PERSPECTIVES: AUTHORIZING THE TRANSPORTATION SECURITY ADMINISTRATION FOR FISCAL YEARS 2012 AND 2013

Tuesday, July 12, 2011

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

The subcommittee met, pursuant to call, at 3:08 p.m., in Room 311, Cannon House Office Building, Hon. Mike Rogers [Chairman of the subcommittee] presiding.

Present: Representatives Rogers, Cravaack, Brooks, and Jackson Lee.

Also present: Representative Clarke of Michigan.

Mr. ROGERS. The Committee on Homeland Security, Subcommittee of Transportation Security, will come to order.

The committee is meeting today to hear different industry perspectives on authorizing the Transportation Security Administration for fiscal years 2012 and 2013.

I would like to welcome everyone here to this hearing and thank all of our witnesses for their patience. I apologize for us being called for votes right when this hearing was supposed to start, but it is what it is. But we look forward to your testimony and greatly appreciate the time and effort you have put into your opening statements and preparing for this hearing. I know the Q&A is going to be very worthwhile.

As many of you already know, this year the committee plans to develop a TSA authorization bill which is intended to enhance and streamline TSA's transportation security initiatives. A few weeks ago, Administrator Pistole testified in front of this subcommittee to discuss his priorities. The purpose of today's hearing is to hear different industry perspectives on the on-going challenges in securing transportation systems and what improvements could be made through the legislative process.

TSA plays a critical role in keeping America's travellers safe. However, its success hinges on the cooperation and support of its public- and private-sector partners. We look forward to continuing this conversation and hearing from some of the diverse groups of public- and private-sector partners that TSA relies on to fulfill its mission of protecting our Nation's transportation systems.

An example of the important collaboration between TSA and its partners has been the response to the foiled Yemen Air cargo attack. Since October, TSA has been working with private industry

to develop and implement a short-term security directive to address certain vulnerabilities. While challenges remain, the open lines of communication between TSA and private industry is commendable and should be recognized as such.

Today's hearing is an opportunity for some of TSA's partners, including the rail, trucking, mass transit, pipeline, and aviation sectors, to voice their insights as to how the TSA authorization bill can improve overall transportation security, enhance the effectiveness of TSA's transportation security initiatives, and address inefficiencies that still may exist. I look forward to an open dialogue that will allow those industry partners that interact with TSA on a daily basis the ability to inform this committee in its continued development of the TSA authorization bill.

The committee considered a TSA authorization bill last Congress as well, H.R. 2200, under the Ranking Member Sheila Jackson Lee's leadership. I look forward to continuing to work with her on a bipartisan basis through this effort.

With that, I now recognize the famous Ranking Member, Sheila Jackson Lee, the gentlelady from Texas, for 5 minutes for her opening statement.

Ms. JACKSON LEE. Mr. Chairman, thank you so very much. Again, let me thank you for the cooperation that we have promoted on this issue of transportation security.

To the witnesses who are here, let me thank you very much for your presence and take note of the fact of Members' schedules that were skewed somewhat because of the long list of votes and may be delaying some Members or cause some Members to have some additional scheduling concerns. So let me just thank you again.

The Chairman is right; we listened to Administrator Pistole, and we now want to listen to the stakeholders. Rail workers, transit security professionals, pilots, and flight attendants are just a few of the many professionals who find it within their job description the responsibility of securing our Nation's railroads, skies, and pipelines against terrorist attacks, including chiefs of metropolitan rail systems, are all at the front lines.

When we talk about security, we are really talking about people. The critical question for me then is, are transportation workers in this country trained and equipped to recognize and mitigate a potential terrorist act? Let me say, just as I did in our first hearing on TSA authorization last month with Administrator Pistole, that we simply cannot forget the lessons learned from the past as we look to preventing future terrorist attacks.

I think the Chairman and I agree that there are many tools. We happen to be unified in our support on canines. Canine is not present at the table today, so we won't ask any questions. But what we are saying is that we need tools, we need professionals persons used to canines, we need persons who are professionals who are used to finding those threats that will impact the American people.

As a Congress and as a Nation, we have taken many steps to shore up the vulnerabilities in protocols and processes that enabled the 9/11 hijackers to penetrate the system and destroy thousands of lives. We have made great progress. We decided to move away from a system with various security companies operating check-

point security to a Federalized system of professional screeners who can quickly adapt to threats based upon the latest intelligence. We implemented mandatory screening for explosives, for checked bags and cargo on passenger planes. We directed that cockpit doors be strengthened, and we deployed more air marshals to secure the aircraft cabin on high-risk flights. Frankly, I am a supporter of increasing those air marshals on our flights internationally.

However, Mr. Chairman, our work is not done, and to the witnesses, our work is not done. Just this year alone, there have been at least five incidents where a flight attendant has had to subdue a passenger to secure the aircraft cabin. I request to submit a list of these incidents for the record, Mr. Chairman.

Mr. ROGERS. Without objection.

[The information follows:]

2011 IN-FLIGHT INCIDENTS INVOLVING FLIGHT ATTENDANTS

UNITED AIRLINES FLIGHT 990

On June 1, 2011 Government and airline officials stated that a United Airlines plane with 144 people aboard returned to Washington-Dulles International Airport for an emergency landing after a fight broke out between passengers. FAA spokeswoman Laura Brown says Flight 990 bound for Accra, Ghana returned to Dulles after a passenger lowered his seat and a passenger behind him objected. Fighter Jets from Andrews Air Force Base, Maryland, were confirmed to have escorted the flight back to Dulles. United Airlines spokesman Mike Trevino stated that "the Boeing 767 dumped fuel as a safety precaution to lighten its weight on landing."

AMERICAN AIRLINES FLIGHT 1561

On Sunday May 8, 2011 on a late flight from Chicago to San Francisco, passengers helped subdue a man whom authorities say was pounding on the cockpit door during the flight. After banging on the cockpit door and shouting during the flight, Rageit Almurisi, 28, was pinned down by two flight attendants and two Air Marshals. Many aboard the flight, airline attendees and security officials believe Almurisi had mental issues.

CONTINENTAL AIRLINES FLIGHT 546

On Sunday May 8, 2011 on a flight from Houston to Chicago there was an emergency landing in St. Louis, after Reynel Alcaide, a 34-year-old passenger, attempted to open a plane exit door. Alcaide has been charged with causing a disruption on board. Authorities believe this was a suicidal attempt. Passengers subdued the suspect until the safe landing was reached.

DELTA AIRLINES FLIGHT 1102

On Tuesday May 10, 2011 a passenger became disruptive and attempted to open an emergency door on a flight from Orlando to Boston but was subdued by passengers. The flight landed safely at Boston Logan International Airport late Tuesday night. An off-duty police officer on board assisted the crew in subduing the passenger and got the situation under control quickly, according to airline officials.

DELTA AIRLINES FLIGHT 413

Olajide Oluwaseun Noibi, 24, a Nigerian-born man who was found with the stolen ID and up to 10 old boarding passes containing various names, was arrested Wednesday June 28 after attempting to board a flight from Los Angeles to Atlanta; 5 days after passing through layers of airport security at New York's JFK airport to board a plane with a day-old boarding pass, Federal authorities said. It is unclear how Noibi managed to get through security at both airports, and whether he left the L.A. airport once flight 415 landed last week and when he attempted to board Delta Airlines flight 46 to Atlanta Wednesday, although he claims to have cleared security. Noibi was charged with being a stowaway aboard an aircraft, according to FBI Special Agent Kevin R. Hogg. He is being held at a Los Angeles Metropolitan Detention Center and appeared in court on July 1.

Ms. JACKSON LEE. While these were not terrorist incidents, they reveal how important a layer of security the flight crews represent. In fact, all of us who fly to work, as I tell my elementary school children as I visit our schools, when I tell them that I fly to work, depend upon those frontline but non-armed flight attendants, along with our pilots, once those doors are closed.

In the last Congress when we passed our bipartisan TSA authorization bill, H.R. 2200, we recognized this and included provisions to improve TSA oversight of air carriers' basic security programs and directed that TSA work with the industry to implement accessible, advanced security training for flight attendants.

Let me be very clear: The airlines need to pay for flight attendant security training, and it needs to be part of their compensation package, on the airlines' package. Please recognize you have the passengers in your hands.

I continue to support these concepts and continue not to understand opposition to improving aircraft cabin security. As we reinforce the pilot door, as we have provided for pilots to carry arms if trained, let us do something for our flight attendants. With a small investment in time and training, we can take the next step in aircraft cabin security by ensuring that the cabin crew are fully trained to meet today's very real threat.

Let us not forget that when you are in the air, when there are no air marshals on board, it is the flight crew that is the very last line of defense. Let's let them work together, air marshals and flight attendants and our very able pilot force.

I say again, nearly 10 years later, let us not forget the lessons learned from 9/11 as we look to addressing the persistent and evolving terrorist threat. Would we, in fact, be even having a discussion on crew training on September 12, 2001? For instance, how many lives were saved when crew and passengers foiled the hijackers on United Flight 93—although, of course, they lost their lives—sending it into the ground in Pennsylvania at 580 miles an hour, sacrificing themselves instead of allowing the terrorists to kill thousands more. I simply say, let us not be pennywise and pound-foolish when it comes to security.

Regarding mass transit and pipeline security, I have introduced H.R. 1900, the Surface Transportation Mass Security Act, which establishes the Surface Transportation Inspection Office and the Surface Transportation Advisory Committee for stakeholder consultation on security programs.

I look forward to working with the Chairman and his leadership on this issue. I might say that H.R. 1900 also would increase the number of canine teams for transit security purposes, for wherever I go, canines come up as a viable tool to be utilized in security.

Let's be creative. Let's move forward in training flight attendants, increasing professionalism, and using the tools that are helpful. Given the consistent threat to our transportation systems, as evidenced by information made public following the demise of bin Laden, we simply must bring our surface transportation efforts in line with aviation. I urge the majority to consider this bill and to be part of the overall TSA authorization.

Finally, Mr. Chairman, I have requested a field hearing on pipeline security, and I know that we are in discussion. I thank you

very much for your interest. I hope that we will have one in Washington, as well. This is a serious matter, and it is reflected by recent incidents in Montana.

I believe we can work together on issues of transportation, pipeline security, both aviation and rail and all aspects of it. It is important to hear from the stakeholders who are here. Again, let me thank you so much very much for being part of America's security. Let's overcome some of our disagreements and follow through on behalf of the American people in securing the homeland.

I yield back, Mr. Chairman. Thank you very much.

Mr. ROGERS. I thank the gentlelady.

I would like to remind other Members that if they have opening statements, they may be submitted for the record.

At this time, I would like to, without objection, ask unanimous consent to insert into the hearing record statements from the Air Forwarders Association, the Aircraft Owners and Pilots Association, the Air Line Pilots Association, the National Air Carrier Association, and the Chamber of Commerce of the United States of America.

Hearing no objection, so ordered.

[The statements follow:]

LETTER FROM THE AIRFORWARDERS ASSOCIATION

JULY 11, 2011.

The Honorable MIKE ROGERS,
Chair, Subcommittee on Transportation Security, Committee on Homeland Security, U.S. House of Representatives, Washington, DC 20510.

The Honorable SHEILA JACKSON LEE,
Ranking Member, Subcommittee on Transportation Security, Committee on Homeland Security, U.S. House of Representatives,Washington, DC 20510.

DEAR CHAIRMAN ROGERS AND RANKING MEMBER JACKSON LEE: The Airforwarders Association (AfA), the voice of the freight forwarding industry representing nearly 400 dues-paying member companies with 3,000 facilities and 20,000 employees, respectfully submits the following comments in advance of the July 12 hearing on industry perspectives on TSA reauthorization. Our members are directly and indirectly regulated by TSA and must work with inspectors, compliance officers and senior officials on a daily basis. As such, AfA applauds the committee's efforts to reduce redundancy, improve efficiencies, and encourage collaboration with the private sector.

The Airforwarders Association is committed to improving aviation security and understands that the seriousness of the recent threats necessitates a change in TSA policies. This commitment drives our recommendations, which will improve security and eliminate redundancies in TSA's air cargo security policies.

These areas of improvement AfA are:

Harmonization of Domestic Security Programs.—TSA has worked diligently in partnership with CBP, as well as FDA and other agencies to better understand security procedures or authorized agent protocols. However, this understanding has yet to lead to action by TSA or other agencies their security practices.

Recommendations:

1. TSA reauthorization should eliminate the inefficient and costly practice of registering authorized agents by each forwarder that may require their services. Oftentimes, such agents are already known in the system due to their work with many forwarders. Requiring reregistration of the same agent is an expensive and redundant security procedure. Forwarders are concerned about the costs to their business as well as the "passed on" cost to their customers in this volatile economy. Once an agent is deemed to be "known" and passes the necessary security checks, forwarders should no longer be required to re-enter them into the system.
2. TSA reauthorization should include the *Modern Credentialing Act of 2011* (H.R. 1690). This legislation is effective in achieving the goal of harmonizing redundant Government credentialing. AfA supports H.R. 1690. This would lower

costs for businesses, as only one credential would have to be issued per employee or agent.

3. CBP, TSA, and the FDA should work together to harmonize supply chain security standards, audits, and applications so that all agencies together can leverage the strength and membership of their existing programs, and decrease unnecessary redundancy for the private sector.

Advancement of National Air Cargo Security Programs with Other Nations.—TSA has worked diligently with our international partners to reach agreements on security protocols. However, this multilateral diplomatic effort is not swift enough to include the majority of cargo passing through the global supply chain en route to the United States.

Recommendations:

1. TSA should continue to aggressively review existing security programs, including screening technologies and policies like Known Consignor, and identify points of commonality to streamline the international screening process. TSA should approve other Nation's security programs and immediately list the locations where a level of security commensurate to domestic cargo screening can be verified.

2. TSA must be directed to harmonize security standards and programs. For example, several European nations are using pallet-screening technologies that have met security standards within their nation. These methods should be recognized and approved by TSA for a limited duration of time leading up to and beyond the 2011 deadline to ensure cargo continues to move efficiently through the supply chain.

Expansion of Existing CBP/TSA Pilot Program on Screening.—Advanced data entry efforts are an important element of a threat-based security program. Current efforts to gather advance predeparture information have been largely successful because of the cooperative engagement that all sides have displayed in the early stages of the pilot program with CBP. AfA has been working closely with CBP to provide feedback and encourage additional participants in the program. The pilot program that has been established has led to positive outcomes already, and the alliance should only get stronger.

Recommendations:

1. TSA and CBP should continue to move forward on the existing pilot program and expand invitations to other forwarders and carriers to participate. Congress should retain robust oversight and be briefed regularly on the status of the program, its successes and policy recommendations gained from the pilot.

Improvement of Inspector Training.—AfA members often deal directly with TSA inspectors in their facilities, where their security, personnel, compliance, and other areas are observed. TSA inspectors can issue guidance or penalize facilities. Compliance and enforcement are necessary and important aspects of a strong cargo security program. However, variations in training (or a lack of any formal training at all) have led to inconsistent interpretations of regulations resulting in unnecessary or inappropriate financial penalties and disruption in small businesses.

Recommendations:

1. All TSA cargo inspectors should complete a mandatory training course prior to engaging in field work. At one time, a training manual was available for inspectors; it is our understanding this was pulled out of circulation.

2. Inspectors should engage in regular retraining to remain up-to-date with new regulations, interpretations from the regional and National TSA offices and the changing security environment.

Formalization of Stakeholder Engagement.—AfA has worked in partnership with the air cargo security team at TSA since the agency was established by the 9/11 legislation. In this time, we have found TSA officials to be sincere in their efforts to facilitate two-way communication with the air cargo industry. AfA has also been a member of the Aviation Security Advisory Council (ASAC) since its inception; ASAC has served a valuable role in bringing private-sector concerns and solutions to the forefront. Friday's announcement that ASAC was being re-established and will report to the TSA Administrator is welcome news.

Recommendations:

1. Congress should closely assess the re-establishment process. It is our hope and belief that original members with a key constituency, like AfA, will remain included in ASAC. Moreover, the previous meetings of ASAC were inconsistent

and ad hoc. We recommend considering a requirement on a minimum number of meetings per year to ensure feedback is regularly submitted to the agency.

Expansion of Canine Detection Units in Pallet Screening.—AfA advocated for the broad definition of screening, which includes multiple methods and offers the greatest flexibility while improving security. As such, AfA supports greater utilization of all screening methods, including Third-Party Explosive Detection Canines (EDCs). TSA has successfully deployed TSA-owned EDC Teams to conduct thorough, timely, pallet-level screening to meet the 9/11 Act mandates. EDC has been shown to provide highly accurate and efficient screening of cargo at the pallet level (indeed, the only efficient pallet screening method currently available and certified by TSA), thereby reducing the cost, time, and operational impacts associated with "de-palletization" and "re-palletization" of cargo.

Recommendations:

1. AfA supports establishing standards for private-sector, third-party EDC teams.
2. TSA should provide access to their TSA-owned EDC training center for testing and certification of private sector dogs.

Fast-Tracking Technology Research and Certifications.—As AfA has previously discussed with the committee, there are two difficulties in TSA's current approach to certifying technology used for cargo screening, as part of the Certified Cargo Screening Program (CCSP). The first is the lack of certification for pallet screening technologies. The second concern of forwarders engaged or desiring to become a CCSF is the lack of "guarantees" given by TSA. Screening technology is a formidable financial expenditure for forwarders and TSA has been unwilling to provide assurances that current certified technologies will still be approved in the future. This uncertainty has surely limited forwarder participation in CCSP.

Recommendations:

1. While AfA supports a policy that approves only technology that is effective and provides security, there are several pallet screening machines in use in the United Kingdom and European Union. We urge Congress to continue to investigate why these technologies are not approved in the United States and to require TSA to focus on pallet screening technologies in the R&D appropriations.
2. TSA should improve the speed of reviews and certifications of all new, novel technologies currently in review by the R&D department.
3. TSA should provide extended "good until" dates on all technology currently certified. In order to improve efficiencies in screening, we recommend a period between 3 to 5 years.

The Airforwarders Association looks forward to continuing our dialogue on these issues with the committee.

BRANDON FRIED,
Executive Director, Airforwarders Association.

STATEMENT OF THE AIRCRAFT OWNERS AND PILOTS ASSOCIATION

JULY 12, 2011

The Aircraft Owners and Pilots Association (AOPA) is a not-for-profit individual membership organization representing more than 400,000 members. AOPA's mission is to effectively represent the interests of its members as aircraft owners and pilots concerning the economy, safety, utility, and popularity of flight in general aviation (GA) aircraft. Each year, 170 million passengers fly using personal aviation, the equivalent of one of the Nation's major airlines, contributing more than $150 billion to U.S. economic output, directly or indirectly, and employing nearly 1.3 million people whose collective annual earnings exceed $53 billion. AOPA respectfully submits the following recommendations in an effort to strengthen physical and economic security while promoting the mobility and economic growth of general aviation.

TSA ISSUED AIRPORT SECURITY DIRECTIVE (SD)

On December 10, 2008, TSA issued Security Directive (SD) 1542–04–08F (SD–08F) to commercial service airports. The SD requires Security Threat Assessments (STA) to be conducted on an expanded airport population including all general aviation owners and operators. Additionally, the SD requires all persons with regular and frequent access to the Air Operations Area to meet the same requirements as

persons with access to commercial aircraft. The Security Directive changed many provisions of existing TSA regulations outside the normal regulatory process, bypassing critical input and comment from impacted parties. This change was an abuse of the SD process which was established to address specific threats of a finite duration. This change has resulted in a patchwork of non-compatible procedures being implemented at airports Nation-wide that have the potential to significantly harm general aviation operators and the commercial service airports where they are based. It has also resulted in concerns and unanswered requests for guidance for transient pilots, especially those landing after hours. Furthermore, security directives are distributed as security sensitive information (SSI), limited to only the regulated entities and those the TSA believe have a "need to know". This has caused a lack of communication and misunderstanding for airport tenants, flight schools, transient pilots, and maintenance providers at airports with commercial airline service.

Many of the obstacles and problems with the regulatory changes in the Security Directive could have been avoided had the TSA chosen to implement them using the Federal rulemaking process, allowing those most familiar with the intricacies of general aviation operations to provide their comments. Because of the seriousness of the aforementioned issues, we would like to see the TSA initiate the required rulemaking process to implement a change of this scope. Our group understands the need to secure America's airports and stands ready to participate fully with the TSA in developing sensible security regulations that will prevent unauthorized access to aircraft and airport facilities.

THE ALIEN FLIGHT STUDENT PROGRAM (AFSP)

The Alien Flight Student Program was established giving the responsibility for background checks of aliens seeking flight training to DRS and the Transportation Security Administration. While AOPA understands the reasons that led to this rule and the efforts by TSA to streamline the process and procedures being utilized, problems nonetheless remain and place an unnecessary burden on the flight training industry. In particular, TSA's Security Regulations governing "Flight Schools" has imposed for several years a requirement that individual flight instructors certificated by the FAA receive initial and annual security awareness training. The FAA imposes on these same flight instructors a requirement for the periodic renewal of their flight instructor certificates. A commonly used method of meeting the FAA requirement is the successful completion within the past 24 calendar months of an approved flight instructor refresher course consisting of ground training or flight training. The AOPA Foundation has for some time been conducting such refresher courses. These two requirements, imposed on the same flight instructors, have timing limitations that do not mesh, imposing a burden on most flight instructors to attend two different training sessions when both requirements could be satisfied in a single extended training session, without serious derogation to aviation security or safety. It is recommended that the TSA rule be amended to allow the requirement for security awareness training to be satisfied at an FAA-approved flight instructor refresher course. This would modestly extend the period of effectiveness of the TSA training received from 1 to 2 years, but would also ensure compliance of the security awareness training requirement by all active flight instructors.

AVIATION SECURITY AS A RISK-BASED, MULTI-AGENCY INITIATIVE

Aviation and airspace security in the years since 9/11 has evolved into a complex layered approach that relies on numerous Federal, State, local, and private organizations, each with unique roles and responsibilities. AOPA supports Administrator Pistole and his intelligence-driven, risk-based approach to counterterrorism protection of our transportation system. The Administrator fully understands that a one-size-fits-all approach to aviation and airspace security is ineffective and often counterproductive. Airspace restrictions, Temporary Flight Rules, and their impact on the National Airspace System must be carefully balanced against the risk and adjusted or modified to reflect changes in the threat, developments in technology, or actionable intelligence. AOPA urges the TSA to address aviation security initiatives from a risk-based, multi-agency perspective and it is essential to engage the general aviation industry in the development and implementation of aviation and airspace security initiatives.

GREATER INDUSTRY PARTICIPATION IN PROCESS DEVELOPMENT

Many of the TSA's current policies, regulations, and procedures that have been implemented in aviation security were hastily drafted and have dramatically changed the security landscape of general aviation and the aviation sector as a

whole. Industry experts were excluded from the process as the discussions and debates began to take on a more law enforcement-centric approach to aviation security. Involvement of industry experts early on in the rulemaking process and on a regular and frequent basis would ensure workable solutions to aviation security problems and add the private sector as a true partner in the prevention, mitigation, and response process.

AIRPORT WATCH PROGRAM

AOPA worked in conjunction with TSA to launch a program that uses America's more than 615,000 pilots as the eyes and ears for observing and reporting suspicious activity at our Nation's airports. Airport Watch is modeled after the highly successful "Neighborhood Watch" program and the initiative has been hailed by Members of Congress and the TSA as a blueprint for Government-industry participation. In recent years funding for this program has been curtailed and a renewed emphasis should be placed on reinvigorating the program and expanding its scope.

AOPA is committed to ensuring the security and economic viability of our Nation's aviation transportation system. We thank you for your time and consideration and look forward to working with the subcommittee in the future.

LETTER FROM THE AIR LINE PILOTS ASSOCIATION, INTERNATIONAL

JULY 12, 2011.

The Honorable MICHAEL ROGERS,
Chairman, House Subcommittee on Transportation Security, H2–176 Ford House Office Building, Washington, DC 20515.

The Honorable SHEILA JACKSON LEE,
Ranking Member, House Subcommittee on Transportation Security, H2–117 Ford House Office Building, Washington, DC 20515.

DEAR CHAIRMAN ROGERS AND RANKING MEMBER JACKSON LEE: On behalf of 53,000 pilot members who fly for 39 airlines in the United States and Canada, the Air Line Pilots Association, International (ALPA) would like to provide you with the aviation security concerns that ALPA believes should be brought to the subcommittee's attention during its hearing on *Industry Perspectives: Authorizing the Transportation Security Administration for Fiscal Years 2012 and 2013.*

Threat-Based Security

The attempted bombing of Northwest (NWA) flight No. 253 on Christmas day, 2009 served as a catalyst for ALPA to publish its white paper: *Meeting Today's Aviation Security Needs: A Call to Action for a Trust-Based Security System,* in January 2010 (attached).* In that paper, ALPA articulated its belief that the Transportation Security Administration (TSA) needed to change its post-9/11 philosophy of screening all people equally for harmful objects to one that focused on identifying individuals having evil intent.

We are pleased to acknowledge the positive response from a number of industry partners, as well as from TSA leadership, expressing agreement with our call for a philosophical change in underlying aviation security philosophy. ALPA has been encouraged by support from TSA Administrator John Pistole, and his call for the implementation of "risk-mitigation" security procedures, as well as his public statements that a pilot flying an airliner should not be required to undergo the same screening procedures as an unknown passenger. TSA's support for the ALPA-conceived alternative screening program for pilots known as CrewPASS, and its evolution into the TSA-endorsed Known Crewmember (KCM) program has been a welcome change to previous "one-size-fits-all" screening requirements.

We believe that initial steps have been taken by TSA to implement more risk-based solutions to securing the aviation sector, and look forward to working with our government and industry partners to continue the expansion of KCM and the creation of other threat-based, risk mitigation programs throughout the aviation security environment.

Federal Flight Deck Officer (FFDO) Program

The FFDO program, using Federally-credentialed, armed pilots trained and managed by the Federal Air Marshal Service (FAMS) to serve as the "last line of defense" of the flight deck, has dramatically increased in size since its inception in 2003. Unfortunately, TSA has not requested or received any significant increase in

*The information has been retained in committee files.

program funding since 2004. FFDO funding remains stagnant with an annual budget of $22.5 million. Because this funding level is inadequate to support the maintenance needs of the existing FFDO force and accommodate processing new candidates, TSA/FAMS ceased accepting new applications in 2011 and has announced its inability to accept applications to the program during 2012, as well.

The FFDO program has been acknowledged by industry and Government to be an extremely successful and cost-effective layer of aviation security. Due to its funding deficiencies, however, coupled with the inadequate number of FAMS fulltime employees (FTEs) assigned to manage the program, it is one of the most under-appreciated, under-utilized, cost-effective security programs implemented since the 9/11 attack on our homeland. We respectfully submit that the FFDO program is in need of a significant increase in funding and managerial oversight, and that Congressional action is needed to bring about such change.

Threatened Airspace Management (TAM)

The failed attack against NWA flight No. 253 also demonstrated deficiencies in ground-to-air communications during or following a significant in-flight security event. Pilots in command of other aircraft, either airborne or about to take-off, were not advised, real-time, of the circumstances impacting NWA–253. This lack of communications deprived these other aircraft commanders, in their role as In-Flight Security Coordinators (ISCs), of critical information which related to a potential security threat to their own flights, and negatively impacted the ability of flight and cabin crewmembers to best protect their passengers and aircraft.

On April 7, 2010 the FAA and TSA did a better job of communicating information to other aircraft regarding an on-going security incident involving a diplomat suspected to be assembling a bomb while in the lavatory of an airliner traveling from Washington, DC to Denver, CO. But even then, the flight decks of only selected airborne aircraft were notified of the event. Since then, we have not witnessed the sharing of security-related information with aircraft commanders that would be of value to them in fulfilling their duties as pilots-in-command.

As recently as June 19, 2011, a bomb threat was made against a Dayton, Ohio to Washington, DC-bound airliner while it was in flight. The captain was not notified of the potential danger until landing at Ronald Reagan National Airport. The aircraft, with its 44 passengers and 3 crewmembers still on-board, sat on the ground for 29 minutes before emergency responders arrived at the plane and the passengers and crew were allowed to deplane.

In addition to this communications deficiency, we have seen no evidence of a clearly-defined, prioritized plan to control the National air space (NAS) in the event of another 9/11-type attack. The U.S. economy and the domestic aviation industry cannot sustain the negative financial impact resulting from a repeat of a Nationwide shutdown as occurred at that time.

ALPA urges the Congress to ensure the development of a prioritized plan for control of the NAS in such circumstances, with the intent of preventing a total or substantial closure.

All-cargo Airline Operations

In November 2010 law enforcement and intelligence agencies interdicted attempts to bomb two U.S. all-cargo aircraft destined from international locations to the United States. Successful detonation of the explosives, hidden in printer cartridges shipped from Yemen, could have resulted in catastrophic loss of life and the aircraft involved.

These attacks confirmed that all-cargo carriers remain a focus of terrorists. Notwithstanding Government and industry awareness of a variety of security vulnerabilities which still exist in the air cargo domain, all-cargo operations remain exempt from a number of security practices mandated for passenger air carriers. Examples include: No hardened flight deck door requirement; no mandated All-Cargo Common Strategy training for crewmembers; no requirement for fingerprint-based criminal history record checks for persons with unescorted access privileges to aircraft and cargo, and no uniform requirement for SIDA restrictions on all-cargo air operations areas.

Although the *Air Cargo Security Requirements; Final Rule,* published in May 2006, did much to improve the security of all-cargo aircraft and operations, it fell short of the mark in a number of critical aspects. A recent investigative report issued by the Government Accountability Office (GAO) on June 20, 2011 provides evidence of a number of these remaining vulnerabilities and bolsters ALPA's argument that much work remains to be done in this regard. Based on the unwillingness of regulators Government and industry to adequately address these deficiencies, we believe that Congressional action is required to bring about needed change.

ALPA is grateful for the subcommittee's attention to these critical transportation security matters and thanks the committee for its leadership in this regard. We look forward to working with you as you craft a TSA reauthorization bill.

Respectfully,

LEE MOAK,
President.

STATEMENT OF NATIONAL AIR CARRIER ASSOCIATION

JULY 12, 2011

National Air Carrier Association (NACA) appreciates the opportunity to submit written testimony on the occasion of the hearing held on July 12, 2011, before the House Homeland Security Committee's Subcommittee on Transportation Security to consider the authorization of the Transportation Security Administration (TSA) for fiscal years 2012 and 2013.

NACA was founded in 1962. Its 17 current member carriers are: Air Transport International, Allegiant Air, Atlas Air, Evergreen Airlines, Kalitta Air, Lynden Air Cargo, Miami Air, National Airlines, North American Airlines, Northern Air Cargo, Omni Air International, Ryan Air International, Southern Air, Sun Country Airlines, USA 3000 Airlines, USA Jet, and World Airways.

All NACA carriers are certificated under Title 14 Code of Federal Regulations Part 121. They are a diverse group of air carriers, providing non-scheduled and scheduled passenger and cargo services. NACA members fill a unique niche in the air carrier industry, offering services in response to ever-changing demands by the travelling public and businesses.

NACA carriers are significant partners with the U.S. Department of Defense (DOD) in the Civil Reserve Air Fleet (CRAF) program. NACA airlines currently carry nearly 95% of the military passengers around the world and 40% of the military cargo.

We appreciate the subcommittee seeking industry views regarding authorization for TSA. Aviation security is a tremendously important facet in the operation of a commercial airline. Al-Qaeda and its affiliates have continued to show an affinity for attacks on the aviation system. Recent news reports and open-source intelligence indicate terrorists are seeking the ability to conduct new attacks involving body IED's that can evade current screening technology. It is critical for the aviation industry and TSA to work closely together to create, deploy, and maintain risk-based layered protections that maximize security against these evolving threats. NACA strongly agrees with Administrator John Pistole that a risk-based approach to airline and airport security is the most cost-efficient and effective means of mitigating the various threats facing the aviation industry.

On June 2, 2011, Administrator Pistole testified before this subcommittee specifically on TSA's efforts regarding risked based security: "TSA has 2 implemented an effective and dynamic security system in the aviation domain consisting of multiple layers of risk-based measures. In the aviation arena, our security approach begins well in advance of a traveler's arrival at an airport, with our vetting programs and intelligence analysts, cargo and compliance inspectors ensuring that airport security plans are followed, and our law enforcement and intelligence community partners working to detect, deter, and prevent terrorist plots before they happen. The security system continues at the airport, including, but not limited to, the work of our Behavior Detection Officers (BDO); Transportation Security Officers (TSO) and the technology that supports the screening of passengers and baggage; Bomb Appraisal Officers (BAO); and canine teams, as well as our partnerships with local law enforcement. In flight, thousands of Federal Air Marshals (FAM) and Federal Flight Deck Officers (FFDO) protect the traveling public."

The broad array of capabilities and resources are designed to fill any holes by coordinating multiple layers of technological and physical security that exists throughout the system. NACA members endorse this approach to ensure our aviation security system is strong, economical, and flexible.

With the subcommittee and full committee considering the development of a full Department of Homeland Security (DHS) reauthorization bill, there is at least one area for which we ask Members of Congress to make a change to public law.

Commercial air carriers providing private charter services must now use their own flight crews or a TSA-certified private screening company to screen sports and other private charters. There are times when commercial charter carriers would like to use on duty TSA screeners to clear passengers and baggage onto the aircraft. Carriers would pay TSA for such services rendered.

This issue has long been a problem for commercial charter carriers. The Federal Aviation Administration (FAA) requires virtually anyone who has contact with the aircraft to be a part of the carrier's Drug and Alcohol Abatement Program (D&O Program) or be covered by an FAA-certified program of their own. When private charters are performed on short notice, commercial charter carriers have extremely limited options for screening the operation as they are unable to bring on off-duty TSA screeners onto their D&O Program on short notice. It is also too expensive to bring a private screening company out to a small airport, which requires long transit times.

NACA and its member carriers believe the best way to solve this problem is to utilize on-duty TSA screeners who are covered by DHS's/TSA's drug abatement program.

The program would work as follows:

1. Commercial air carrier submits a request to the Federal Security Director (FSD) at the airport of departure and requests the use of on-duty TSA screeners to conduct the screening of passengers and baggage for charter flight;
2. Screeners are provided if FSD has personnel available for the requested time;
3. TSA bills the air carrier for the use of the screeners at the regular hourly rate plus any overtime chargers that may apply.

TSA does not believe it has the statutory authority to charge air carriers for this requested service. TSA must be granted the authority to charge air carriers for the use of on-duty screeners when requested (and available).

NACA and its member carriers respectfully request the Homeland Security Committee include language in the Chairman's mark that would: (1) Permit TSA screeners to conduct screening of passengers and baggage for commercial air carrier charter flights, and, (2) permit TSA to charge the air carrier the regular hourly rate plus any overtime charges for providing such screening service.

We now offer a comment on a matter of broader TSA policy. The working relationship between the aviation industry and TSA has continued to evolve since the agency was created in 2001. We believe, however, there is always room for improvement that reflects the costs of implementing security measures and the highest value of threat detection, as well as countermeasures that add tangible value to our security efforts.

NACA believes the subcommittee, and Congress as a whole, needs to conduct stronger oversight of the TSA and its possible promulgations of new regulations without industry input.

TSA regularly issues Security Directives (SDs) to the commercial aviation industry in response to real-time intelligence suggesting an 'imminent' threat. SDs have an immediate or short-notice compliance date assigned to them that mandate actions—often obtaining certain equipment, changes in procedures, or restrictions on operations. TSA rarely seeks industry input regarding how operations will be impacted due to the issuance of an SD. TSA seems surprised when industry has logistical problems with implementation after it imposes an SD. Some issues could be worked out with minimal notice (a few hours) to industry and granting it the ability to provide comment.

This lack of consultation on the pre-issuance of SD's has created the impression that TSA uses SD's to bypass the normal rulemaking process, which relies on industry comment and participation to craft the best rule. We urge the subcommittee to examine TSA's use of SD's and test whether rules are being set that would more properly be the subject of a rulemaking.

We appreciate the committee's consideration of these requests. Having the flexibility to use on-duty TSA screeners in certain situations will provide tremendous economic value and flexibility to the commercial charter carriers in this difficult business environment. NACA also believes the subcommittee would benefit by learning about TSA's system of issuing SD's and how that process has evolved. We stand ready to work with you on this and all other enhancements to our aviation security system.

In closing, National Air Carrier Association and its 17 member airlines are committed to working closely with TSA, intelligence agencies, and Congress in developing the best possible aviation security system.

LETTER FROM R. BRUCE JOSTEN, EXECUTIVE VICE PRESIDENT, GOVERNMENT AFFAIRS, CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA

JULY 12, 2011.

The Honorable MIKE ROGERS,
Chairman, Subcommittee on Transportation Security, Committee on Homeland Security, U.S. House of Representatives, Washington, DC 20515.

The Honorable SHEILA JACKSON LEE,
Ranking Member, Subcommittee on Transportation Security, Committee on Homeland Security, U.S. House of Representatives, Washington, DC 20515.

DEAR CHAIRMAN ROGERS AND RANKING MEMBER JACKSON LEE: The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than 3 million businesses and organizations of every size, sector, and region, submits this letter in advance of your hearing entitled "Industry Perspectives: Authorizing the Transportation Security Administration for Fiscal 2012 and 2013," and the Chamber commends your leadership in addressing these important issues that impact the security and economic competitiveness of the United States.

We offer these recommendations in the spirit of cooperation and will continue to work with the subcommittee on a bipartisan basis to solve these important issues.

Redundant Credentialing Process

Congress should strive to remove unnecessary burdens on American businesses. The Transportation Security Administration (TSA) should move forward with harmonizing redundant government credentialing requirements. The Transportation Worker Identification Credential (TWIC) and the Hazmat Endorsement (HME) are redundant credentials administered by TSA. Both programs query the same databases for criminal, immigration, and other violations, utilizing the same disqualifying criteria, appeal, and waiver processes. Yet, transportation workers must pay: $94 for a HME to carry hazmat; $132.50 for a TWIC to enter the ports; $50 for a FAST card at the border; and $27 for a Security Identification Display Area (SIDA) badge at each airport for a total cost of $303.50.

The Chamber believes that the redundant fees and background checks of U.S. transportation workers is an unnecessary cost for businesses. These sentiments are echoed by the U.S. Small Business Administration, which added the TSA's inaction in implementing Section 1556 to its Regulatory Review and Reform (r3) program's Top 10 list of most egregious regulations on small businesses.

H.R. 1690, the "Modern Credentialing Act of 2011" would achieve the goal of harmonizing redundant Government credentialing. The Chamber would support H.R. 1690 and encourages its inclusion in the TSA Authorization Bill.

Aviation Security Advisory Committee

All of TSA's regulatory action and inherent functions have a dramatic impact on the private sector. Whether TSA is screening passengers or air cargo, their activities and mandates significantly hinder travel and tourism, and the domestic and global supply chain. A more effective and efficient TSA would have a positive impact on the global competitiveness of U.S. industry globally.

However, TSA has no formal advisory committee where the private sector can engage in discussions regarding TSA policy. The Commercial Operations Advisory Committee (COAC) reports to the Commissioner of U.S. Customs and Border Protection (CBP) and the Secretary of the U.S. Department of Treasury. The Chamber believes that a similar committee reporting directly to the Administrator of TSA would be an effective mechanism to ensure that private sector opinions are considered in policy development.

While H.R. 1447, the Aviation Security Stakeholder Participation Act of 2011, is a partial step toward this goal, we recommend that the Aviation Security Advisory Committee (ASAC) report directly to the Administrator of TSA. It is essential to the effectiveness of such a committee that agency leadership is engaged in regular discussions with industry stakeholders.

Furthermore, such legislation should not specify a subcommittee structure. Members of the ASAC should be permitted to establish subcommittees relevant to current issues at the beginning of their term in office. Should these changes be made, the Chamber would support H.R. 1447, and would recommend that it be included in the broader TSA Authorization legislation.

Multilayered Risk-Based Approach to Security

The Chamber supports Administrator Pistole's efforts to develop the agency into a risk-based, intelligence-driven counterterrorism agency dedicated to protecting the transportation system. We agree that a multilayered risk-based approach is the

most effective way to ensure security and facilitate legitimate trade and travel. The TSA Authorization bill should facilitate these risk-based methods. The Chamber urges the subcommittee to stand firm in support of risk-based approach and reject any 100 percent mandates.

Air Cargo Security

The Chamber has been encouraged by the work among the private sector, CBP, and TSA in reaction to recent terrorist attempts on air cargo planes. Efforts to gather advance predeparture information have been largely successful because of this cooperative engagement. The established pilot program has already led to positive outcomes, and the alliance should only get stronger.

The collective reaction to these terrorist attempts is a model for how Government and the private sector can work together to secure the supply chain, without having a detrimental impact on business operations. Rather than push for more regulation or legislation, the Chamber supports the current pilot program and its gradual expansion to more carriers.

Next Generation Global Supply Chain Security

The Chamber supports trusted shipper programs, which encourage security investment while providing strong trade facilitation benefits to members. These programs help focus limited resources on high-risk shipments, and should be developed further.

However, the subcommittee should consider ways to harmonize and streamline existing U.S. and international programs. For example, there are striking similarities between CBP's Customs-Trade Partnership Against Terrorism, TSA's Certified Cargo Screening Program (CCSP), and the Food and Drug Administration (FDA) is also developing their own trusted shipper program. International equivalent programs also exist such as Canada's Partners in Protection (PIP) or the internationally recognized Authorized Economic Operator (AEO).

All of these programs focus on the same mission, and have similar mandates. Yet, rather than cooperate with applications, audits, and other requirements, U.S. Government agencies appears to be siloed in their approach. CBP, TSA, and the FDA should work together to harmonize supply chain security standards, audits, and applications so that all agencies together can leverage the strength and membership of their existing programs, and decrease unnecessary redundancy for the private sector.

Harmonizing and streamlining would help TSA efforts to reach the 100 percent screening mandate for international in-bound passenger flights. Greater focus should be given to seeking harmonization with international screening methods and international supply chain security programs. Rather than creating new and redundant screening programs, the TSA should work with their international counterparts, to leverage the strength of existing programs. This effort would ensure that resources are being used to improve security rather than being focused on redundant screening methods.

Canine Inspection Programs

Industry shares the mission and goal of TSA to ensure the safe and secure transport of cargo throughout the supply chain. Companies have invested heavily in equipment, training, labor, and screening technicians to administer the various screening programs, to meet new security program requirements and to comply with emergency-based security directives. The tight timelines for screening, increased volumes from an economy emerging from economic recession, and lack of screening alternatives have strained the private sector's ability to efficiently and effectively meet the goal of securing the supply chain.

To best utilize the flexibility in the 9/11 Act and assist industry in meeting the common security goals, the Chamber urges greater utilization of all screening methods, including Third-Party Explosive Detection Canines (EDCs). Canines were specifically included in the 9/11 Act as an authorized screening method, and TSA has successfully deployed TSA-owned EDC Teams to conduct thorough, timely, pallet-level screening to meet the 9/11 Act mandates. EDC has been shown to provide highly accurate and efficient screening of cargo at the pallet level, thereby reducing the cost, time, and operational impacts associated with "de-palletization" and "repalletization" of cargo.

With third-party EDC teams currently used to protect many Federal facilities and screen cargo bound for the United States on commercial ships and some air cargo locations, the Chamber supports standards for private sector, third-party EDC teams. Further, TSA should provide access to their TSA-owned EDC training center for testing and certification of private sector dogs. Finally, the Chamber encourages TSA to consider greater harmonization and mutual recognition of internationally

certified EDC teams to help address the challenge of screening the high-risk air cargo bound for the United States at or before the point of departure.

The Chamber remains committed to ensuring that the United States remains secure, and prosperous. We look forward to working with the subcommittee on this important legislation.

Sincerely,

R. BRUCE JOSTEN.

Mr. ROGERS. We are pleased to have several distinguished witnesses——

Ms. JACKSON LEE. Mr. Chairman, if I might, I have a unanimous consent request.

Mr. ROGERS. Please.

Ms. JACKSON LEE. I would ask unanimous consent that the gentleman from Michigan, a Member of the full committee, Mr. Clarke, be authorized to sit for the purpose of questioning witnesses during the hearing today.

Mr. ROGERS. So ordered.

Ms. JACKSON LEE. Thank you.

Mr. ROGERS. We have several distinguished witnesses before us today on this important topic.

Let me remind the witnesses that their entire statements will be submitted for the record. So if you would like to summarize those, we will get through the panel as quickly as possible and get to the questions.

First, we have Mr. Tom Farmer, who currently serves as the assistant VP at the Association of American Railroads. I have enjoyed working with him during my tenure and am proud to have him on the panel.

The floor is yours, Mr. Farmer.

STATEMENT OF THOMAS L. FARMER, ASSISTANT VICE PRESIDENT FOR SECURITY, SAFETY, AND OPERATIONS, ASSOCIATION OF AMERICAN RAILROADS

Mr. FARMER. Thank you, sir, very much.

Mr. Chairman, Ranking Member Jackson Lee, Members of the committee, on behalf of the Association of American Railroads, thank you very much for this opportunity to appear today.

At the outset, I must emphasize that nothing is more important to railroads than the safety of their employees—safety and security of their employees, of their operations, and of the communities that they serve.

As all of you know, the issue of rail security garnered significant attention in early May with the reporting on al-Qaeda interest in attacking trains following the operation in Abbottabad, Pakistan, that ended with the demise of Osama bin Laden. The reference to railroads as a potential terrorist target is not surprising, however. Indeed, the extensive efforts that we, as an industry, have devoted to rail security enhancement since the 9/11 attacks have been premised very much on this reality.

Immediately following 9/11, acting on their own initiative, freight railroads formed a top-level security task force, consisting of more than 150 industry experts, to conduct a thorough evaluation of risk and security in the rail network. Key focus areas included critical infrastructure, freight rail operations, hazardous materials, communications and control systems, and military shipments.

This effort produced the rail industry's "Terrorism Risk Analysis and Security Management Plan." It is a comprehensive, priority-based blueprint of actions that the industry developed to deal with the new realities. This plan was adopted by the industry in December 2001, within just 3 months of the 9/11 attacks. It remains the foundation of our security efforts today, updated as necessary based on experience in its usage and on changing circumstances with the threat.

The plan defines four progressively higher-security alert levels and details a series of actions to be taken at each level. There are more than 50 permanent countermeasures that were implemented as a result of the development of this plan. In addition, those areas that those countermeasures cover focus upon expanding the skills of our people, the effectiveness of our procedures, and the use and the protection of technology. In addition to regular exercises conducted both industry-wide and by individual railroads, we test the effectiveness of this plan under realistic terrorism prevention and response scenarios.

A particular area of emphasis in what we do is intelligence and security information. The railroads maintain for this purpose the Surface Transportation Information Sharing and Analysis Center and the Railway Alert Network, and these two entities work in concert to provide effective means for timely notification of security threats, incidents, and other emergencies, to assure daily security awareness, and to expand the understanding of terrorist tactics.

One of the key initiatives of these two bodies, in partnership with the American Public Transportation Association, is a daily brief called the "Transit and Rail Intelligence Awareness Daily." This product is a very concise overview of the most significant matters of the day in the areas of suspicious-activity reporting, terrorism analysis, general security awareness, and cybersecurity. The information provided by this means can be used by railroads to augment training and awareness briefings for employees. It can also be shared with local, State, and Federal authorities to expand partnerships.

Now, the railroads set as a top priority working closely with TSA and other Federal components to enhance our collective effectiveness and security. In the written testimony, there are several areas we address of concern. There are three I would like to highlight here.

First, as we approach the 10th anniversary of the 9/11 attacks, the timing is right for a thorough review of rail security strategy and programs. What are we doing? Why? How can we be more effective in a sustainable way? The objective is agreed security priorities that set the framework for how we measure the effectiveness of our policies, our programs, and our initiatives. TSA's freight rail division, very much to its credit, has agreed to meet with the railroads for this purpose next month.

Second, we need better information sharing between the railroads and the Government agencies we work with. Railroads provide a wealth of security-related information every day to various Government entities, but we get too little back that helps us perform the security mission effectively.

We have submitted to TSA and DHS an intelligence requirement to close this gap, one that is focused on looking for in-depth analysis of the preparatory actions that terrorists take—in successful attacks, that they have tried in foiled plots, they tried in failed attempts—looking for insights into the mindset and the thinking of the adversary, how they function, to enable better-informed and more effective security measures.

Third, the railroads believe that security and efficiency would be enhanced if there were more consistency and standardization in TSA's inspection activities, especially in the interpretation of TSA's security regulations. Inconsistencies among field offices and departures from the priorities and policies set by TSA headquarters are causing adverse but avoidable impacts on rail operations. We believe that the TSA regional security inspectors that have been appointed as liaison to the Class I railroads and to Amtrak offer a viable and a sustainable solution to these concerns.

I thank you for this unique privilege, and I am very happy to answer any questions you may have.

[The statement of Mr. Farmer follows:]

PREPARED STATEMENT OF THOMAS L. FARMER

JULY 12, 2011

On behalf of the members of the Association of American Railroads (AAR), thank you for the opportunity to appear before the committee and discuss the reauthorization of the Transportation Security Administration (TSA) and rail security issues generally. In freight rail, AAR members account for 72 percent of track mileage, 92 percent of the industry's employees, and 95 percent of revenue. North American freight railroads provide the vital link for goods and commodities used by industries and consumers throughout the continent and in the global market. Indeed, one-third of all U.S. exports are transported by rail at some point en route to their destinations world-wide. Amtrak, America's National passenger railroad, is a member of AAR, as are several commuter railroads. A joint Freight and Passenger Coordinating Committee established by AAR provides a forum to advance an integrated approach on matters relating to rail safety, operations, and security.

OVERVIEW OF THE RAIL INDUSTRY SECURITY PROGRAM

The Industry Commitment. Safety and security are top priorities for railroads, freight and passenger, for their employees, for their operations, and for the communities they serve. In early May, following the raid that resulted in the killing of Osama bin Laden and the seizure of a high volume of materials on al-Qaeda's operational status and plans—an achievement for which all involved in the United States Government and military deserve the highest commendation—widespread media reporting focused on a document indicating al-Qaeda interest as of February 2010 in attacking trains, potentially in connection with the tenth anniversary of the terrorist attacks on the United States on September 11, 2001. This revelation produced a unique opportunity—insight into the adversary's thinking, gained from a place believed impregnable to intrusion or seizure. However, al-Qaeda's inclusion of rail as a target is not surprising. The extensive efforts devoted to security enhancement since the 9/11 attacks, by the railroads at their initiative and by the Federal security and intelligence agencies, have been premised on this reality.

In the immediate aftermath of those attacks, a security task force consisting of some 150 officials representing railroads, supported by experts in security and intelligence, conducted a comprehensive risk assessment with the objective of developing an industry-wide security plan. Using National intelligence community best practices, five critical action teams scrutinized different aspects of the railroad system: hazardous materials transport; rail operations; critical infrastructure; information technology and communications; and military movements. Collectively, this analysis examined and prioritized railroad assets, evaluated potential vulnerabilities, and assessed threats, and then identified a range of countermeasures.

This effort culminated in December 2001 with issuance of the Terrorism Risk Analysis and Security Management Plan, a comprehensive, priority-based blueprint

of actions that remains the foundation for the industry's proactive, coordinated approach and for individual railroads' security programs. The plan included more than 50 permanent security-enhancing countermeasures that were immediately implemented and provided for elevated security based on increases in the terrorist threat.

Continuous Improvement. But no one is resting on laurels. The Class I railroads, and many regional and short-line carriers, have adapted the plan to their unique operating circumstances. Implementation of the plan is exercised on a recurring basis—by railroads individually and collectively as an industry on an annual basis. These exercises appraise the effectiveness of the industry's security plan in realistic terrorism prevention and response scenarios. The most recent industry-wide exercise occurred on October 15, 2010; the next is scheduled for October 13, 2011. For this year's event, we have invited direct participation by Federal entities—TSA, DHS, FBI, and the Federal Railroad Administration (FRA)—specifically to assure effective implementation of an efficient, understandable, and sustainable process for sharing of intelligence on security threats and incidents with the rail industry, freight and passenger.

The industry security plan is regularly evaluated and modified as needed to ensure maximum continued effectiveness. Lessons learned from exercises and experiences in actual security-related incidents inform reviews and updates of the plan with the specific purpose of assuring its viability to meet changing threat circumstances. A comprehensive review completed in 2009 evaluated the plan's guiding assumptions, risk methodology, and countermeasures, yielding an updated version that took effect in November of that year. Indeed, railroads—in conjunction with the TSA, other Federal security partners, rail customers, and others—are constantly evaluating approaches to further enhance rail security as part of a continuous improvement process.

Persistent Coordination. An integral element of this effort is the Rail Security Working Committee, supported by AAR's security staff. Reporting to the railroads' chief operating officers in the industry's Safety and Operation Management Committee, the Security Committee consists of senior executives, security officials, and police chiefs with our member railroads, coordinates the overall rail industry security effort, and reflects the industry's on-going commitment to work in a coordinated fashion, amongst railroads and with government agencies at all levels. Through monthly consultations, the committee identifies issues of concern, develops and coordinates implementation of solutions, and presents proposals for coordinated effort with the Federal Government. The committee also participates in joint security coordination meetings with TSA's Freight Rail Division under the Intermodal Security Training and Exercise Program (I–STEP). These sessions sustain constructive relationships and effective communication between the railroads' security and law enforcement officials and their counterparts in TSA, DHS's Office of Infrastructure Protection, FRA, and the FBI. The I–STEP forum allows for open and candid discussion of current programs and initiatives, future priorities, and prevailing security issues and concerns.

Information Sharing. Essential to success in the security mission is timely access to accurate and relevant intelligence and security information—an area on which the rail industry security committee places particular emphasis. To sustain effectiveness, the railroads maintain two standing capabilities focused on the railroads security information needs—the Surface Transportation Information Sharing and Analysis Center (ST–ISAC) and the Railway Alert Network—and assign highly experienced liaison officers with the FBI's National Joint Terrorism Task Force and Southwest Border Joint Terrorism Task Force.

Originally established in the 1990s in coordination with the Department of Transportation, the ST–ISAC applies analytical expertise for threats and security incidents that either affect or have significant implications for critical infrastructure, physical and cyber. Working in secure facilities, the ST–ISAC taps a broad range of sources daily, including analytical products from the Federal Government (classified and unclassified), to develop and disseminate material to aid in the protection of physical assets and information technology networks and systems. Especially noteworthy are the ISAC's efforts in cybersecurity. Each day the ISAC issues multiple advisories to the railroads each day addressing potential vulnerabilities in specific software or equipment and providing guidance on protective measures. This material directly supports the extensive and effective cybersecurity programs maintained by the major railroads. A standing Rail Information Security Committee provides a forum for regular consultations amongst professionals across the industry and a mechanism for the sharing of effective security practices.

The Railway Alert Network (RAN) serves as the security information center for the rail industry, focused on providing immediate alert notification of serious incidents and emergencies and on analysis of the implications to freight and passenger

railroads of intelligence and security information relating to threats, incidents, suspicious activity, and terrorists' capabilities, tactics, and techniques. Functioning within a secure facility with classified communications capabilities, the RAN performs a daily review of information from a broad range of sources for relevance to rail and homeland security. Targeted security information and awareness messages are developed for the railroads and shared with security partners in their operating areas at the local, State, and Federal levels.

A particularly noteworthy initiative is the Transit and Rail Intelligence Awareness Daily (TRIAD), produced jointly with the American Public Transportation Association (APTA), the ST–ISAC, and the Public Transit Information Sharing and Analysis Center (PT–ISAC). TSA supports this cooperative effort through a joint information sharing working group and funding of the PT–ISAC, pursuant to the authorization of section 1410 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Act). The purpose of TRIAD is to present the most significant matters of the day in the areas of suspicious activity and incident reporting, counterterrorism analysis, general security awareness, and cybersecurity. The target audience is senior executives, and security and law enforcement officials with railroads and mass transit agencies and local, State, Federal, and private sector security partners.

Partnership for Security. Maintaining a constructive relationship with TSA is a top priority of the rail security effort. In 2006, both the freight railroads and passenger railroads, the latter in conjunction with mass transit agencies, agreed with TSA on a series of security action items and on inspection of the effectiveness of their implementation by TSA Transportation Security Inspectors—Surface. The action items focus on areas foundational to an effective security program—planning, training, exercises, physical security, information security, personnel security, means to raise security posture in response to threats, and related matters. The cooperative program proved quite effective. For passenger railroads and transit agencies, TSA gained a wealth of information on security posture that informed program development, grant program priorities and awards, and identification of "smart security practices." In freight rail, the demonstrably successful partnership produced substantial reduction of risk associated with transport of toxic inhalation hazardous (TIH) materials. For the DHS Annual Performance Report (2008–2010), TSA reported a 53.6% reduction in risk as of the end of 2008 against the baseline defined in 2006. Significantly, all of this risk reduction, which exceeded the 50% target set by TSA, occurred under the agreed action items, without regulatory compulsion. AS of 2010, TSA reports "an industry-wide risk reduction variance of 95.73% against the original 2005/2006 baseline." Again, the measures and procedures that made this significant achievement possible predated the promulgation of the Rail Transportation Security Rule (49 CFR Part 1580), their having been implemented by the railroads either on their own initiative pursuant to the industry security plan or to meet the agreed security action items.

Complimenting this progress are cooperative efforts with emergency responders in local communities to enhance awareness and elevate preparedness to respond to hazardous materials (HAZMAT) emergencies. These initiatives include funded, in-depth, hands-on training under realistic conditions for first responders at the Security and Emergency Management Training Center, a component of the rail industry's Transportation Technology Center, Inc., in Pueblo, CO. This premier first responder training center is a member of FEMA's National Domestic Preparedness Consortium. Individual railroads conduct training programs and joint exercises with local and regional emergency response units as well.

The rail industry remains committed to cooperative efforts with the Federal Government for sustainable security enhancement. In this context, there are several areas that warrant attention.

ISSUES OF SECURITY CONCERN TO THE RAILROADS

Rail Security Strategy. We are approaching the 10th anniversary of the 9/11 attacks. The timing is opportune for a thorough review of the strategy and programs for rail security generally (freight and passenger). What are we doing? Why are we doing it? What are the core priorities? How can we be more efficient and effective? TSA's Freight Rail Division has agreed to discuss these issues at a meeting to be held next month.

Intelligence Support for Rail Security. The foundation for the effectiveness of any security strategy is intelligence. On multiple occasions since May 2010, the rail industry has submitted, separately to DHS and to TSA, a priority intelligence requirement seeking expansion of the depth of analysis of past terrorist attacks, attempts, and plots targeting rail. The objective is to know what we can know—as fully as

possible—through in-depth analysis of the preparatory actions in successful terrorist attacks, failed attempts, and foiled plots that have targeted rail. The purpose: To draw insights into the mindset and thinking of the adversary, of how terrorist operatives function, and thereby enable better informed and more effective security measures.

DHS and FBI intelligence products commonly reference the Terrorist Planning Cycle as a means to "assist organizations with their development and implementation of protective measures to deter, detect, disrupt, and defend against attacks from both domestic and international terrorists." Substance needs to be added to this good advice. For rail security, this substance entails a breakdown against each phase of the cycle, in as much detail as the available information allows, of the known or inferred elements of target selection, planning, preparation, and execution, either by single operations targeting rail or by a composite analysis of multiple such operations. With preparatory and execution activities so delineated, opportunities can be identified where particular types of security measures and activities may prove effective in deterrence or disruption. In essence, we are seeking to expand the concept of "actionable intelligence" to include analysis that creates opportunities for security.

Rail Security Inspection Activities. In multiple forums over an extended period, the railroads have expressed concern with inspection activities by TSA's Transportation Security Inspectors—Surface. The industry's principal concern is the inconsistency and lack of standardization in inspectors' interpretations of TSA's security regulations and expectations regarding rail security in general. There are disparities between the policies and guidelines set by TSA's Freight Rail Division and the actions of surface inspectors in the field. Actions accepted by some TSA field offices result in official citations as violations by others. Another problem is repeated bypassing of the communication and coordination process—with the Rail Security Coordinators (RSCs)—appointed pursuant to TSA regulations. TSA, and other DHS components, sometimes directly engage with rail employees in the field, who often lack the authority and means to address the issues raised by the inspectors.

AAR believes the Regional Security Inspectors (RSIs) appointed as liaison to the Class I railroads and Amtrak offer a viable and sustainable means to resolve these concerns. However, organizationally they are not in the chain of command of the surface inspectors in the field. Yet, the official correspondence sent to the railroads that announced the appointment of the RSIs defines a scope of authority and responsibility well-tailored to attaining this objective. Key points from these letters include:

- "the RSIs–Surface will act as the points of contact for the Class 1 and Regional Railroads";
- "to ensure consistent application of regulations both nationally and across a railroad's operating system";
- "coordinate TSA field activities . . . to minimize negative impact on your railroad operations"; and
- "use your new RSI–Surface to the fullest extent."

Substantively engaged, consistent with the above commitments, we do believe the RSIs can bring about greater consistency and standardization in inspection priorities and activities, with benefits for the Government in quality of results and for the railroads in operational efficiency. Further, this approach can assure early and efficient resolution of issues of security concern—using the communications process TSA has established by regulation and expressly referenced in the RSIs' appointment letters.

Effective Deployment of Visible Intermodal Prevention and Response (VIPR) Teams. The rail industry acknowledges the potential value of the VIPR program's random and unpredictable security measures for deterrence and disruption of terrorist planning and preparations. Indeed, some railroads, passenger and freight, have hosted deployments and derived substantial benefits from the visible security enhancement. Across the industry, however, inconsistency in the implementation of this program remains a significant concern—in management (conflicts and duplications between TSA field offices) and in execution of operations (continuing instances of inadequate notice to and coordination with railroads on operations). For mass transit and passenger rail, TSA abides by agreed protocols for notice, coordination, planning, preparation, execution, and after-action review. A similar approach should be used for the rail industry as a whole. Fundamental aspects of the program should include:

- Prior notice to the railroad by TSA of all proposed VIPR deployments at least 2 weeks in advance, unless a credible threat or other emergency circumstances dictate otherwise.

- Joint development by TSA and the affected railroad(s) of the operations plan for each VIPR deployment or group of deployments.
- Integration of local law enforcement in the VIPR deployment(s) to foster informed partnerships and elevated preparedness for joint security enhancement actions.
- Clearly stated risk-based justifications for the deployments.

Analysis and Use of Reports on Significant Security Concerns Submitted to the TSA Freedom Center (TSOC). The Rail Transportation Security Rule, at 49 CFR section 1580.105 for freight railroads and 49 CFR section 1580.203 for passenger railroads, requires the reporting of significant security concerns to the TSA Freedom Center. To date, despite its substantial volume, this reporting has not produced consistent analysis for trends of concern in rail security or for educative value from the security awareness and heightened vigilance perspective. However, the Freedom Center does widely disseminate the railroads' reports to an extensive audience of Federal, State, and local government officials, selected public transportation authorities, and other private sector representatives. The criteria for this distribution are unclear, as many recipients have no responsibilities for rail security. Meanwhile, the railroads do not receive directly the TSOC reports or any significant feedback on the analysis or implications of the reports they submit. Yet, this reporting does create an opportunity to identify potentially "high value" information, discern developing trends of potential concern or their absence, and disseminate analyses that will inform steps to elevate preparedness and capabilities to prevent and immediately respond to acts of terrorism. A consistent process would enable a continuing educational opportunity for application by railroads in their efforts to assure continuous vigilance and security awareness. The existing intelligence and security information dissemination process maintained through the Railway Alert Network (RAN) would assure distribution of these analytical products to appropriate officials with railroads nationally, freight and passenger.

Flexibility in Grant Investments to Expedite Security Solutions. DHS manages a wide range of grant programs aimed at enhancing capabilities to prevent, respond to, and recover from acts of terrorism and natural disasters. Often, investments in these capabilities yield benefits for resiliency that offer advantages in both categories of risk. Unfortunately, however, the rules associated with these grant programs frequently impose limitations on the ability to apply them in effective ways for expedited and sustainable solutions. As all of these programs aim to achieve a similar purpose, the guiding principle should be: Enable the grants to solve the most pressing problems instead of allowing program rules to limit the problems that can be solved. Wherever practicable, the benefits of unity of effort and economies of scale should inform decisions on funding for projects. As a representative example, TSA's Freight Rail Division has worked in coordination with the railroads to complete vulnerability assessments on more than 70 rail bridges in the Western Rivers System—principally crossings of the Mississippi, Missouri, and Ohio rivers. The resulting reports make recommendations on mitigation measures, ranking the bridges in priority. A composite approach to Federal support through grant funding of bridge-hardening projects—drawing upon not just the Freight Rail Security Grant Program but also the State Homeland Security Grant Program, the Urban Area Security Initiative where applicable, the Transit Security and Intercity Passenger Rail Security Grant Programs for structures with passenger train service, and the Port Security Grant Program—can expedite redress of the potential security concerns identified in the assessment process.

To TSA's credit, significantly broader flexibility has been shown in the outreach forums to grant-eligible entities for the fiscal year 2011 cycle. Support has been expressed for composite projects, both those integrating different functional areas, such as a single application seeking funding of technological enhancements and operational activities to enhance security at a critical rail station, and those that offer the potential to link funds from the Freight and Transit Security Grant Programs. We hope this positive trend continues.

Commuter Rail Security Enhancement. As noted at the outset, AAR has established a joint Freight and Passenger Rail Coordinating Committee to foster sustained, cooperative effort on issues of security concern. Major terrorist attacks overseas have targeted commuter trains in major cities, with the bombings in Madrid (2004) and Mumbai (2006) as dramatic examples. In the United States, commuter rail has been the subject of threats, notably the expressed interest in targeting commuter trains revealed in November 2008. A collaborative project, integrating Government and industry, focused on development of a sustainable security enhancement strategy for commuter rail would provide substantial benefits. This effort should combine varied joint operations with local law enforcement departments and

testing of tailored security technologies, with resource support from security grant allocations.

CONCLUSION

Assuring the security of the Nation's passenger and freight railroads requires a multi-faceted, cooperative effort that taps the full range capabilities—in the private sector and at all levels of government—and applies them to best effect to assure preparedness and enhance capabilities to prevent and respond to acts of terrorism.

Our Nation's railroads look forward to working with policymakers and others in a true public-private partnership to see that this objective is met successfully.

Mr. ROGERS. Thank you, Mr. Farmer, for your testimony. We appreciate you being here and know your time is valuable and it took a lot of time to prepare for that. So I appreciate that.

Our second witness is Martin Rojas. He is the vice president of the American Trucking Association.

The Chairman now recognizes Mr. Rojas for your opening statement.

STATEMENT OF MARTIN ROJAS, VICE PRESIDENT FOR SECURITY AND OPERATIONS, AMERICAN TRUCKING ASSOCIATION

Mr. ROJAS. Thank you very much, Mr. Chairman. It is a pleasure to be here again.

Chairman Rogers, Ranking Member Jackson Lee, and Members of committee, thank you for the opportunity to testify today on the authorization of the Transportation Security Administration.

The trucking industry is an integral component of our economy, earning more than 80 percent of all domestic freight revenues. It is important to note that the trucking industry is comprised primarily of small businesses, with 97 percent of trucking companies operating 20 trucks or less. In addition, 80 percent of all U.S. communities depend solely on trucks to deliver and supply their essential everyday commodities.

Because trucking is such a vital link in our economy, it is critical that Government requirements improve security without curtailing our ability to deliver America's freight efficiently and safely.

As this committee is aware, since the terrorist attacks of 9/11 Government agencies have implemented various security initiatives impacting the transportation sector as a whole. In today's multimodal, intermodal transportation system, this means that a requirement on one specific mode can indirectly impact the operations of other modes. This is certainly the case in the trucking industry, considering that trucks and commercial drivers operative at maritime facilities, rail yards, airports, chemical facilities, and across our Nation's international borders.

To mitigate the risk of future terrorist attacks and to ensure both our National security and our economic security, ATA agrees with the recent statements by TSA Assistant Secretary John Pistole. In early June, Mr. Pistole testified that we must reduce the vulnerabilities in our transportation system by establishing risk-based approaches and by using sound intelligence in making decisions and in carrying out our operations. The trucking industry favors such an approach.

As this committee considers how to improve the security of the country's transportation system, ATA suggests the following four observations:

First, mandating more security requirements does not necessarily improve the security of the transportation system. As an industry already heavily regulated by safety and security requirements, more regulations will only increase the compliance burden on trucking companies, rather than improve security. From multiple background checks and security plans to overlapping security training and en route security, the trucking industry is already saturated by such requirements.

Second, ATA encourages improving Government/industry information sharing. Trucking companies have embraced several initiatives by law enforcement agencies and the intelligence community to exchange and better understand our mutual information needs to improve our Nation's security. Today, ATA members are involved in various programs including with the Director of National Intelligence, the FBI's InfraGuard Program and its Domestic Security Alliance Council, as well as the Homeland Security Information Network. ATA believes that enhancing information-sharing efforts at the Federal, State, and local level will improve the security posture of the trucking industry.

Third, Government agencies must continue to improve coordination of their respective security regulations. ATA recognizes that higher-risk operating environments must address specific risks associated with such operations. Because of the differing environments in which trucking companies operate, applying a one-size-fits-all approach is not practical for the trucking industry. However, Federal agencies must improve interagency coordination to establish mechanisms that recognize some basic common requirements or protocols in other security programs. Complying with multiple security requirements by various Government agencies is simply not suitable for motor carriers.

Last, ATA believes that the TWIC Reader Rule must be finalized and the program's application process must be improved. TSA and the U.S. Coast Guard must finalize the TWIC Reader Rule and ensure that the processes and systems are hardened to prevent counterfeiting and the use of false identity information to obtain a real TWIC.

ATA still believes that the TWIC should function as a single security threat assessment and credential that satisfies the background check requirement of multiple programs. In this regard, I want to thank again this committee's bipartisan leadership in addressing the multiplicity of background checks and credentials. ATA is a strong supporter of the Modern Security Credentials Act of 2011, and we look forward to this bill becoming law.

On behalf of ATA and its members, I thank you for the opportunity to share some comments, and I look forward to answering your questions.

[The statement of Mr. Rojas follows:]

PREPARED STATEMENT OF MARTIN ROJAS

JULY 12, 2011

INTRODUCTION

Chairman Rogers, Ranking Member Jackson Lee, and Members of the Subcommittee on Transportation Security, thank you for the opportunity to testify today on the Authorization of the Transportation Security Administration for fiscal year 2012 and 2013. My name is Martin Rojas and I am Vice President for Security and Operations at the American Trucking Associations (ATA). Founded in 1933, ATA is the Nation's preeminent organization representing the interest of the U.S. trucking industry. Directly and through its affiliated organizations, ATA encompasses over 37,000 companies and every type and class of motor carrier operation.

The trucking industry is an integral component of our economy, earning more than 80% of U.S. freight revenues and employing approximately 7 million workers in trucking-related jobs, including over 3 million commercial drivers. It is important to note that the trucking industry is comprised primarily of small businesses, with 97% of trucking companies operating 20 trucks or less, and 90% operating six trucks or less.[1] More importantly, about 80 percent of all U.S. communities depend solely on trucks to deliver and supply their essential commodities.

HIGHWAY SECTOR SUPPORTS STRONG NATIONAL AND ECONOMIC SECURITY

The U.S. highway and motor carrier sector has been defined by the U.S. Department of Homeland Security (DHS) as one of 19 Critical Infrastructures/Key Resources (CI/KR). In 2006, various private sector highway-related organizations established the Highway and Motor Carrier Sector Coordinating Council (SCC). The SCC works in partnership with public sector representatives established under a counterpart Government Coordinating Council (GCC) under the auspices of the Critical Infrastructure Protection Advisory Committee (CIPAC). The SCC and GCC have met for the past 5 years on a quarterly basis to share ideas and exchange information to improve the security of the Nation's highways. In addition to the SCC, ATA and its members participate in many industry and Government-led initiatives focused on enhancing security and ensuring an open and efficient transportation system to deliver America's freight.

Today's hearing takes place just 2 months away from the tenth anniversary of the terrorist attacks of September 11, 2001. Since that day, the United States has undertaken various initiatives, both domestically and abroad, to prevent our enemies from planning and executing further terrorist attacks against us. From sending thousands of heroic men and women to fight abroad, to implementing laws, regulations, and strategies at home to reduce the risk of terrorist attacks on U.S. soil, our country has mobilized an immeasurable amount of public and private resources to defeat our enemies and secure our country. To further mitigate the risks of future attacks, we must continue to strengthen cooperation among Government agencies and private sector entities, improve coordination among Government agencies at the Federal, State, and local level, and we must coordinate closely with our international trade partners and allies. Established by the Homeland Security Act of 2002, DHS absorbed a number of Federal agencies with the overall goal of improving coordination and intelligence sharing under a single Federal entity. One of the main early objectives of DHS was to "unify authority over major Federal security operations related to our borders, territorial waters, and transportation systems."[2] After almost a decade since the 9/11 terrorist attacks, it is appropriate that we review and assess the effectiveness of various security regulations and programs implemented to improve our Nation's security.

IMPLEMENTING MORE SECURITY REGULATIONS DOES NOT INCREASE SECURITY

As a key agency within DHS, TSA can have a positive impact by strengthening the partnership with private sector counterparts instead of seeking to increase the number of security regulations on industry. As a country, we will never fully eliminate the risk and potential for terrorist attacks. But the trucking industry believes that by working together, we can improve our Nation's security posture without sacrificing the need for an efficient and effective transportation system hampered by excessive security regulations and requirements.

---

[1] American Trucking Associations, *American Trucking Trends 2011* (March 2011).

[2] President George W. Bush, "The Department of Homeland Security" Proposal, June 2002, p. 2 *http://www.dhs.gov/xlibrary/assets/book.pdf.*

At a recent hearing before this committee, TSA Assistant Secretary John Pistole stated:

"TSA employs risk-based, intelligence driven operations to prevent terrorist attacks and to reduce the vulnerability of the Nation's transportation system to terrorism . . . TSA works collaboratively with industry partners to develop and implement programs that promote commerce while enhancing security and mitigating the risk to our Nation's transportation system."[3]

ATA fully agrees with Mr. Pistole's approach and stands ready to work with him, his TSA colleagues, and other Federal agencies to improve the security and safety of the transportation sector. As we have encouraged past TSA leaders, we recommend that Mr. Pistole perform a review of all the security regulations and programs throughout the Federal Government that presently affect all transportation modes so that the agency has a better appreciation of the numerous security initiatives in place today. Because of the ubiquitous nature of the trucking industry throughout the transportation system, Government mandates established to improve security in other modes or sectors have both direct and indirect impacts on trucking operations.

As this committee considers the present security challenges faced by the highway transportation sector and how to mitigate these risks, it must also recognize that the trucking industry must also comply with a number of other regulations. In addition to security regulations, the trucking industry faces far-reaching and complex Federal safety regulatory system. Increasing the regulatory burden on trucking companies as they are struggling to recover from the "Great Recession" does not help this critical industry improve its security nor its ability to grow its bottom line to spur economic growth and create more jobs. Since both Government and private sector resources are finite, we must choose carefully how we invest them to ensure our operations are secure, safe, and efficient.

At a hearing held on May 4, ATA expressed its gratitude to committee Members for their efforts and bipartisan leadership in addressing the continued multiplicity of Security Threat Assessments (STAs) that commercial drivers undergo to deliver America's freight. ATA and its members strongly support enacting the MODERN Security Credentials Act of 2011 and we look forward to Congress passing this important legislation. This issue remains ATA's top security policy priority for its potential to bring relief to millions of truck drivers and thousands of trucking companies from unnecessary and overlapping background checks and the resulting excessive costs.

In addition to multiple STAs, there are several Government regulations and programs that require trucking companies to develop security plans, provide security training, develop en-route security procedures and incorporate security designs at company facilities, many with overlapping requirements, including the following:

- *HM–232F*.—The Pipeline and Hazardous Materials Safety Administration (PHMSA), an agency within the U.S. Department of Transportation (DOT), promulgated HM–232 soon after the 9/11 attacks. HM–232 required companies transporting placarded loads of hazardous materials to develop security plans, security awareness training (both general and in depth), and en-route security requirements. In March 2010, PHMSA issued a final rule, HM–232F, refining the list of hazardous materials that require transportation security plans. Carriers that transport this security-sensitive subset of hazardous materials must perform risk assessments of their operations and facilities, as well as provide in-depth security training to employees handling these hazardous materials. The Federal Motor Carrier Safety Administration (FMCSA) assures compliance with HM–232F during regular motor carrier visits where safety and security reviews are conducted. ATA supported PHMSA's rulemaking efforts to establish a risk-based approach to the transportation of hazardous materials.
- *Customs-Trade Partnership Against Terrorism (C–TPAT)*.—U.S. Customs and Border Protection (CBP) worked with industry immediately after the 9/11 attacks to develop a "supply-chain" security program to increase the security of international shipments imported into the United States by all modes of transportation, including trucks. Though C–TPAT is not mandated by statute and remains a "voluntary" security program, most carriers are required to become C–TPAT members by their C–TPAT certified customers/importers with international cross-border shipments from Canada and Mexico. The program requires participating companies to conduct risk-assessments, develop security plans, and implement specific security recommendations made by CBP Supply

[3] Pistole, John S.; Statement before the Subcommittee on Transportation Security, June 2, 2011, p. 1.

Chain Security Specialists (SCSS) to become certified and validated by CBP. As part of the Free and Secure Trade (FAST) program, Canada implemented a parallel program for imports called Partners-In-Protection (PIP) that incorporates similar requirements and a separate application and validation by Canadian officials.

- *Certified Cargo Screening Program (CCSP).*—TSA's CCSP program requires participants to establish personnel security, physical security, and procedural security requirements. The CCSP recognizes other STAs such as the Hazmat Endorsement, the Transportation Worker Identification Credential (TWIC) and the FAST card. As with other programs, CCSP has security requirements that are unique to the air cargo environment regarding technologies for screening cargo as well as chain of custody procedures.

ATA recognizes that higher-risk operating environments, such as air cargo or cross-border operations, have security requirements that must address specific risks associated with such operations. Because of this, a "one-size-fits-all" security approach is not a viable methodology for designing and implementing security requirements for an industry with such diverse operations. However, Federal agencies must improve inter-agency communication and coordination to establish mechanisms that recognize basic "common requirements" in other security programs. In essence, if a CCSP compliant carrier is applying for C–TPAT certification, the carrier's application should undergo an accelerated C–TPAT certification and validation process.

Because several Federal agencies already require motor carriers to implement security measures, the trucking industry does not support Federal agencies, including TSA, implementing additional security regulations. Agencies that are considering implementing security requirements for the transportation of specific types of regulated commodities should first review all three of the above-listed programs—HM–232F, C–TPAT, and CCSP—and consider if those programs meet their requirements for the secure transportation of their regulated commodities.

A positive example of the above scenario has been the implementation of the Chemical Facilities Anti-Terrorism Standards (CFATS) by DHS's Infrastructure Protection (IP) office. In early discussions between IP and transportation industry stakeholders, IP recognized that commercial drivers already undergo various STAs when transporting certain cargo, including chemicals, or when operating in certain environments. Thus, DHS considers the Hazardous Materials Endorsement (HME), TWIC and FAST screenings as compliant with the CFATS background check requirement. DHS also recognized the oversight authority of other Federal agencies over chemical products, including DOT's regulations for the safe and secure transportation of hazardous materials. Thus, DHS stated that CFATS regulations would not supersede other Federal agencies' chemical security requirements.

TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL: FOCUS ON OUTCOME NOT ON OUTPUT

ATA views the TWIC as a single instrument that can satisfy the needs of multiple agencies requiring background checks in various operating environments. The original concept of the TWIC, as espoused as far back as 2003, was to establish a single process, system, and credential with broad application across multiple programs and transportation modes requiring workers to undergo a STA. This concept, known as "enroll once, use many", was included as one of the 20 key recommendations in the Surface Transportation Security Priority Assessment prepared by the Transborder Security Interagency Policy Committee (IPC)[4] with industry input and support.

On May 10, 2011, the Government Accountability Office (GAO) released a study during a hearing held by the Senate Committee on Science, Commerce, and Transportation to review the impact of the TWIC on port security. The GAO report found a number of security concerns with the implementation of the TWIC program, including the use of counterfeit TWICs to gain access to maritime facilities and the use of counterfeit identifications and fake identity data to apply and successfully obtain authentic TWICs. As a result, some Members of Congress are questioning if the TWIC has added any true value to the security of maritime facilities and to the entire transportation sector.

GAO has recommended a number of steps be taken by TSA and the U.S. Coast Guard (USCG), including the need for internal controls and effectiveness assessments to evaluate compliance with the program's original objectives. GAO also suggested that TSA analyze and determine what cost-effective measures can be taken to ensure that the program corrects the specific weaknesses found during the assessments, especially as they relate to identity fraud and the use of counterfeit

[4] National Security Council, The White House, March 2010.

TWICs. As a long-standing member of the TWIC private sector stakeholder group, ATA is concerned about the GAO findings.

As long as TWIC is simply used as a flash-pass it will be no more secure than a driver's license or any other photo identification. ATA urges this committee to ensure TSA and USCG do not delay issuing a Final Rule for TWIC readers so that maritime facilities can use the technology established under the TWIC program to verify the identity of the card holder prior to accessing a facility. The technology embedded in the TWIC and the readers should help deter the use of counterfeit TWICs. TSA and the TWIC contractor must also take the necessary steps to ensure that TWIC applicants are presenting valid identification and biographical data upon application.

INFORMATION SHARING TRUMPS SECURITY REGULATIONS TO FIGHT TERRORISM

Last February, an alert trucking company employee prevented a terrorist plot involving explosives. A visiting Saudi student, Khalid Ali-M Aldawsari, was arrested in Lubbock, Texas for plotting to bomb several locations throughout the State, including the home of former President George W. Bush. Luckily, Mr. Aldawsari was arrested and his plans came to an end.

The incident reflected the positive effects of implementing appropriate security training for employees, while encouraging them to remain alert and report any suspicious activity or other concerns. In this case, a trucking company employee recognized and researched some of the materials listed in a package and alerted the company's security team. Federal law enforcement personnel were brought in and the would-be terrorist was eventually arrested when he tried to pick up the package.

As with other terrorist plots inside the United States, this event garnered much media attention. However, among the various media outlets that covered the story, it was a CNBC story that truly captured the essence of what transpired:

"In the end, it wasn't a TSA agent, a Homeland Security operative or an FBI agent who first spotted alleged terror plotter Khalid Ali-M Aldawsari. It was the employees of a private shipping company. According to the Government, somebody at the shipping company called local police after becoming suspicious about a chemical package that Aldawsari was set to receive.

"Meanwhile, officials at the chemical company that sent the material called the FBI with their suspicions about Aldawsari—and later worked with an FBI agent who posed undercover as a company employee in dealings with the suspect."[5]

What this story highlights is that all of us, Government agencies, private industry, and concerned citizens all share the responsibility for fighting terrorism. In the end, information sharing is the best and strongest tool that we have to stop potential terrorist plots and to fight terrorism at home and abroad.

As this event demonstrates, the private sector is an essential partner and part of the solution for combating terrorism. We don't need more regulation, we need more cooperation.

ATA and its members are presently participating in a number of information-sharing initiatives to facilitate the flow of information and intelligence to improve the security posture of our industry. Initiatives involving the Homeland Security Information Network, the Office of the Director of National Intelligence, the FBI's InfraGard program, as well other Federal, State, and local efforts, are allowing industry to share information directly with the intelligence and law enforcement community. ATA urges this committee to support such exchanges of information as a better alternative to establishing additional security regulations on an industry already over-burdened by safety and security regulatory mandates.

CONCLUSION

In the past 10 years, many legislative, regulatory, and voluntary efforts have been implemented to minimize the threat of another terrorist attack in the United States. Though well-intended, many initiatives have resulted in a multiplicity of overlapping and burdensome security requirements on trucking companies. Unfortunately, rather than augmenting the security of the transportation sector, the focus has been more on regulatory compliance rather than evaluating the impact of existing security requirements.

ATA urges the committee to consider the following recommendations as it deliberates TSA's Authorizations for fiscal year 2012 and 2013:

---

[5] "How Two Companies Stopped a Terror Suspect", CNBC.com; February 24, 2011; *http://m.cnbc.com/us__news/41766933*.

- *Do not mandate more security regulations*.—As an industry already heavily regulated by safety and security requirements, more security regulations will not improve security but will only increase the compliance burden on trucking companies;
- *Encourage information sharing*.—Industry has embraced several initiatives by law enforcement and intelligence agencies to exchange information and increase our mutual understanding and information needs to improve our Nation's security posture;
- *Improve agency coordination*.—Increase the communication and coordination among Federal agencies that have established security requirements and programs that impact the surface transportation sector. TSA's Transportation Sector Network Management (TSNM) could play a role in such an initiative;
- *Ensure the TWIC reader rule is issued promptly*.—TSA and the USCG must finalize the TWIC reader rule and ensure that the processes and systems are hardened to prevent counterfeiting and the use of false identity information to obtain a real TWIC.

Again, on behalf of ATA and its members, I thank you for the opportunity to share some comments regarding our industry's perspective and priorities as this committee considers authorizing TSA for fiscal year 2012 and 2013. I look forward to answering any questions you may have.

Mr. ROGERS. Thank you. Thank you for that remark. The fact is, this issue was brought to the attention of this committee by your association. So I really appreciate the fact you gave us a heads-up and we were able to do something about it.

Our next witness is Chief Wanda Dunham. I am proud of Wanda; she is an alumni of the same university from which I graduated. She is just younger than I am. But it is good to have her here. She is the chief of police for the Metropolitan Atlanta Rapid Transit Authority Police Department. We look forward to hearing her testimony.

I will tell you, Madam Ranking Member, you are going to hear about canines today after all. They have vapor-wake canines in the Atlanta transit system.

Ms. JACKSON LEE. Smart people.

You can advertise your school where you graduated.

Mr. ROGERS. Okay. Jacksonville State University. That is where we went to school.

Chief DUNHAM. That is right.

Mr. ROGERS. The floor is yours.

STATEMENT OF WANDA Y. DUNHAM, ASSISTANT GENERAL MANAGER AND CHIEF OF POLICE AND EMERGENCY MANAGEMENT, METROPOLITAN ATLANTA RAPID TRANSIT AUTHORITY

Chief DUNHAM. Yes, sir.

Good afternoon, Mr. Chairman and distinguished committee Members, and thank you for the opportunity to provide my testimony on behalf of the Metropolitan Atlanta Rapid Transit Authority in Atlanta, Georgia, and as a representative of public transportation systems throughout our Nation.

My name is Wanda Dunham, and I am privileged to serve as the police chief and assistant general manager for police services and emergency management to the ninth-largest public transportation system. I speak to you as someone with more than 24 years of police experience in a mass transit environment and as someone who collaborates with industry as a member of the American Public Transportation Association's—that is "APTA"—Committee on Pub-

lic Safety. Sincerely, I truly appreciate your interest in improving public transportation security across the country.

Today, the Transportation Security Grant Program and other Federal funding programs remain a significant resource in the development and implementation of key countermeasures against terrorist threats. Since 2003, MARTA has received approximately $31 million in Federal funding in support of various target hardening and security initiatives. With the support of this investment, MARTA has been able to develop or expand key programs, such as our CCTV camera system, as well as acquiring 15 bomb-detection canine teams, including three vapor-wake canine teams that can actually detect the presence of odors related to an explosive device.

I would like to spend a few minutes to discuss the canine teams at MARTA. Proudly, I am pleased to report that MARTA has been at the forefront in the use of this unique canine application in the detection of explosive devices. We were the first transit agency to be part of the canine explosives detection program for TSA at Lackland Air Force Base in San Antonio, Texas.

In August 2004, MARTA was asked to participate in a pilot program for the first vapor-wake canine program in the country. This program was spearheaded by the prestigious Auburn University Canine Detection Training Center in Auburn, Alabama. Our canine, Tabby, was the first graduate of this impressive training program. Although Tabby was retired last year, we recognize her today for her 6 years of dedicated service to our department.

While there has been a great degree of progress made at MARTA and other transit systems across the country, there is still much work that is required to continue to keep our Nation safe. Much of the efforts and focus of this investment to date has been in the area of infrastructure and target hardening.

Many transit systems are experiencing the need for additional funding and broader funding guidelines to leverage existing capital investments with operational support. An increase in the limitation on operational funding from 10 percent to 20 percent and allowing personnel costs where the need can be strongly substantiated will be of great support to many transit systems.

Additionally, recent intelligence information has substantiated what we have known for some time: That transit systems remain highly vulnerable for potential attacks. To that point, it is highly recommended that Congress reauthorize the Transit Security Grant Program at levels similar to those authorized under the 9/11 Commission Act.

Finally, I cannot emphasize how important and critical the financial support provided by Congress through the Transit Security Grant Program has been to local and regional efforts across the country in keeping our customers safe. As we prepare at a regional level to ensure we are responsive and prepared for new and emerging 21st-Century security threats, the support of Congress and your continued commitment to keeping stride with the financial needs are vital to our success.

I will entertain any questions. Thank you for your time.

[The statement of Chief Dunham follows:]

PREPARED STATEMENT OF WANDA Y. DUNHAM

JULY 12, 2011

Good afternoon, Mr. Chairman and committee Members, and thank you for the opportunity to provide my testimony on behalf of the Metropolitan Atlanta Rapid Transit Authority, in Atlanta, GA and as a representative of public transportation systems throughout our Nation. My name is Wanda Dunham and I am privileged to serve as the Police Chief and Assistant General Manager, for Police Services and Emergency Management to the 9th largest public transportation system in our great Nation. As you may be aware, MARTA is one of eight identified Tier 1 transit agencies in the Nation, which means that it warrants especially high considerations for security investments. I speak to you as someone with more than 24 years of police experience in a mass transit environment, as a member of the TSA Peer Advisor Group and as someone who collaborates within the industry as a member of the American Public Transportation Association's (APTA) Committee on Public Safety. Sincerely, I truly appreciate your interest in improving public transportation security across the United States. My testimony today is to speak to the growing demand and need for continued homeland security-related investments.

MARTA OVERVIEW

There exists no priority higher than the safety and security of the more than 500,000 unlinked passenger trips we deliver on a daily basis. Our multi-modal transit system includes 48 miles of heavy rail serving 38 stations with 318 railcars and 505 buses on 91 routes. Our rail system, which began service in 1979, has a direct connection to Hartsfield-Jackson International Airport. As MARTA has expanded over the last 3 decades to remain an economic engine for the region, so has our attention to security-related needs and proactive strategies. MARTA is the longest-serving transit police agency in the country designated as a CALEA (The Commission on Accreditation for Law Enforcement)-certified agency. MARTA Police is a full-time, full-service agency with 321 sworn officers including detectives, uniform patrol, and explosive detection units, etc. It is the availability of resources such as the Transit Security Grant Program (TSGP) and a collaborative effort with Federal, State, local agencies and community partners that has allowed MARTA Police to implement multi-level, comprehensive strategies to ensure the safety of our riders. Now, more so than ever, recent events and intelligence regarding terrorist plans reinforces our need to be all the more vigilant and continue to make security-related investments a high National priority.

TSA & MARTA COLLABORATION

The Transit Security Grant Program and other Federal funding programs remain a significant resource in the development and implementation of key countermeasures against terrorist threats. Since 2003, MARTA has received approximately $31 million in Federal funding in support of various target hardening and security initiatives. With the support of this investment, MARTA has been able to develop or expand key programs, such as the following:

- The implementation of Homeland Security CCTV cameras in all 38 stations, with cameras soon to be installed in over 500 buses and 200 railcars.
- Increased access control systems at a number of critical infrastructures.
- Conducted over 10 Homeland Security Emergency and Evaluation Plan (HSEEP)-compliant security exercises within the last 5 years to include various State, local, and Federal partners.
- Enhanced protective measures (e.g., fencing, lighting, barrier gates) at critical and vulnerable infrastructures such as rail yards and bus garages.
- Secured & updated more effective bomb abatement equipment such as a Total Containment Vessel (TCV) and a bomb robot.
- Acquired 15 bomb-detecting canine teams, including 3 "vapor wake" canine teams that can actually detect the presence of odors related to an explosive device.

I would like to spend a few minutes to discuss the canine teams at MARTA. Proudly, I am pleased to report that MARTA has been at the forefront in the use of this unique canine application in the detection of explosive devices. We were the first transit agency to be part of the Canine Explosives Detection program for TSA at Lackland Air Force Base, in San Antonio, Texas. Since our involvement with the TSA canine program, our canine teams have received numerous "Top Dog" recognitions for their exemplary performance. In August 2004, MARTA was asked to participate in a pilot program for the first vapor wake canine program in the country.

This program was spearheaded by the prestigious Auburn University Canine Detection Training Center in Auburn, Alabama. Our canine, Tabbie, was the first graduate of this impressive training program. Although Tabbie was retired last year, we recognize her today for her 6 years of dedicated service to our department. Since the Auburn program's inception, we have had five additional canines who have participated in this exceptional program.

We have discovered that transit riders report feeling safer when Canine Units are present. Their presence and visibility has helped to prevent the introduction of explosive devices and deter criminal activity in the transit system, all the while providing a more secure environment for our customers. I cannot say enough about the TSA Canine Program. TSA is committed to this program and has done an excellent job providing transit agencies such as MARTA with the resources to keep this program viable and accessible to assist in the fight against terror on our systems.

Furthermore, TSA has been responsive to many of our concerns within the transit community. For example, we recognize and appreciate the recent changes to the Transit Security Grant Program guidelines to allow for maintenance and sustainability as allowable expenses, and the revised timeline for the execution of capital projects from 36 to 48 months.

Most recently, the TSA Administrator, John Pistole, visited MARTA to witness first-hand the many effective security measures made possible through TSA grant funding.

OPPORTUNITIES FOR IMPROVEMENT WITH TSGP FUNDING

While there has been a great degree of progress made at MARTA and other transit systems across the country, there is still much work that is required to continue to keep our Nation safe. Much of the effort and focus of the investments to date has been in the area of infrastructure and target hardening. Many transit systems are experiencing the need for additional funding and broader funding guidelines to leverage existing capital investments with operational support. An increase in the limitation on operational funding from 10 percent to 20 percent and allowing personnel cost, where the need can be strongly substantiated, will be of great support to many transit systems. For instance, a COPS program specifically for transit has been a funding proposal strongly supported by other Tier 1 agencies.

Additionally, recent intelligence information has substantiated what we've known for some time; that is, those that mean to do our country harm have not eased up on their determination. In addition, we've also learned that transit systems remain highly vulnerable for potential attacks. To that point, it is highly recommended that Congress reauthorize the TSGP at levels similar to those authorized under the 9/11 Commission Act. The eligible use of funds included in Section 1406(b) of the 9/11 Commission Act should be maintained and broadened. This measure would allow for transit systems to continue to provide security countermeasures at all vulnerable locations at risk of terrorist attack versus having to prioritize vulnerable assets based on funding restrictions.

Furthermore, the ability to communicate and coordinate with other public safety agencies, such as police and fire, is vital to our ability to respond and guard against any perceived or real threats. Legislation in Congress to allocate spectrum to public safety agencies has the potential to further the interoperability challenges among transportation agencies. A change in the definition of public safety in Section 337 is recommended to reflect the need of transit security and emergency services to access the public safety spectrum for emergency service purposes. MARTA also supports the allocation of the 700 MHz spectrum (D–Block) to public safety, if the aforementioned change is made.

Finally, we also urge the committee to support the security legislative recommendations of the American Public Transportation Association, including support for the Public Transportation Information Sharing and Analysis Center (PT–ISAC) and Security Standards programs, which have been submitted to the committee under separate cover.

I cannot emphasize how important and critical the financial support provided by Congress through the TSGP has been to the local and regional efforts across the country in keeping our customers safe. Unfortunately, we cannot say that the threat today is any less than it was 10 years ago. As we prepare at a regional level to ensure we are responsive and prepared for new and emerging 21st Century security threats, the support of Congress and your continued commitment to keep in stride with the financial needs are critical to our success.

CONCLUSION

I appreciate the committee for allowing me to provide testimony on these critical security-related issues. MARTA and our fellow transit agencies look forward to working with you and the Members of the committee as you work to develop this next critical authorization bill. I will be happy to answer any questions at this time.

Mr. ROGERS. Thank you, Chief Dunham.

Our fourth witness, Mr. Raymond Reese, is the corporate health, safety, and security leader for Colonial Pipeline and will be testifying on behalf of the Alabama—Alabama—the Association of Oil Pipe Lines, of which I am sure Alabama is a part.

The Chairman now recognizes Mr. Reese for his testimony.

STATEMENT OF RAYMOND J. REESE, CORPORATE HEALTH, SAFETY, AND SECURITY LEADER, COLONIAL PIPELINE COMPANY, ON BEHALF OF THE ASSOCIATION OF OIL PIPE LINES AND THE AMERICAN PETROLEUM INSTITUTE

Mr. REESE. Thank you, sir. Yes, it is. In fact, we have an asset going through your fine State.

Good afternoon, Chairman Rogers, Ranking Member Jackson Lee, and Members of the subcommittee. My name is Raymond Reese. I am the corporate health, safety, and security leader for Colonial Pipeline. I appreciate the opportunity to appear on behalf of the Association of Oil Pipe Lines, the American Petroleum Institute, and as the chairman of the Oil and Natural Gas Sector Coordinating Council.

America relies on a network of more than 170,000 miles of liquid pipelines to move the energy that fuels our Nation's economy and supports our quality of life. One of these pipelines is Colonial. Colonial is headquartered near Atlanta, Georgia, where we operate a system consisting of 5,500 miles of pipeline. When measured by volume transported, Colonial is the largest refined products pipeline in the world.

Colonial and the pipeline industry are committed to delivering these materials safely and efficiently. We are also committed to keeping our facilities secure. With regard to the security of the pipeline system, the private and public sectors share the same goal: Protecting our facilities from attack so that we can avoid loss of life, disruption of service, damage to assets, injury to our employees or the public, or harm to the environment and National economy.

One key element to effectively managing these risks is what TSA has properly called a partnership between the private and public sectors. The success of this and any partnership is dependent upon communication and collaboration. In my view, the most effective security program will be one that is not static but, rather, constantly adjusting to ensure we are staying ahead of an increasingly sophisticated adversary. Regular interaction with TSA through a strong industry partnership provides this flexibility.

TSA's Pipeline Security Division, or PSD, regularly conducts corporate security reviews of major pipeline operators to assess their security plans, and critical facility inspections of the most sensitive locations in the pipeline industry to focus on implementation of security practices at pipeline facilities. The results of these two reviews have been used to develop security smart practices that are then shared across the industry. I can personally attest to the thor-

ough nature of the CSR review and how extensive some of these on-site visits can be.

TSA has also issued pipeline security guidelines which are specific Federal recommendations for security practices throughout the pipeline industry. These were built on previous guidance and the requirements of the 9/11 Commission Act. Our industry has worked with TSA in the development of these guidelines.

Rarely will industry and regulators agree on every point or proposal. The very nature of effective partnership necessitates some level of mutual compromise. As mentioned, the pipeline industry has a constructive working relationship with PSD. However, we believe there are opportunities for improved communication elsewhere within DHS.

Our industry seeks appropriate risk-tiering for gasoline storage facilities in the CFATS program and a conclusion to a process that has gone on for a very long time. Contrary to initial indications from DHS, CFATS regulations were expanded to include operators of gasoline storage facilities by the incorporation of a flammable-mixtures provision late in the regulatory development process. Comments were filed asking DHS to review the technicalities of its rulemaking, and for over 2 years our industry has awaited a formal reply.

Another concern is with credentialing. The liquid pipeline industry and others within the oil and natural gas sector support effective risk-based security standards of high-risk facilities to protect critical infrastructure. We support credentialing programs that check personally identifiable information against the terrorist screening database.

We are concerned, however, that DHS's proposal for a personal surety program would create significant new administrative burdens with little or no security enhancement. Rather than creating a redundant credentialing program, it would appear more logical for DHS to leverage the already widely accepted and utilized TWIC program.

I want to thank this subcommittee and its members for addressing this issue in your recent markup of H.R. 901. It is our hope that this proposal will be a part of the final CFATS reauthorization this year.

In conclusion, it has been my personal experience that TSA's Pipeline Security Division has assumed a responsible approach to pipeline security, working with industry to identify effective and practical security practices for pipeline operators. In my view, this partnership serves the American public well.

And I thank you for the opportunity to comment, and I look forward to your questions.

[The statement of Mr. Reese follows:]

PREPARED STATEMENT OF RAYMOND J. REESE

JULY 12, 2011

Good afternoon Chairman Rogers and Ranking Member Jackson Lee and Members of the subcommittee, my name is Ray Reese and I am the corporate health, safety, and security leader for Colonial Pipeline. I appreciate this opportunity to appear before the subcommittee today on behalf of the Association of Oil Pipe Lines (AOPL) and the American Petroleum Institute (API). In addition, I serve as the

Chair of the Oil and Natural Gas Sector Coordinating Council (ONG SCC), which I will discuss in further detail below.

Colonial Pipeline is headquartered in suburban Atlanta, Georgia, where we operate a pipeline system consisting of 5,519 miles of pipeline, beginning in Houston and crossing the South and East before terminating at the New York harbor. When measured by volume transported, Colonial is the largest refined products pipeline in the world, daily delivering about 100 million gallons of gasoline, diesel fuel, jet fuel, and home heating oil and fuels for the U.S. military.

AOPL is an incorporated trade association representing 49 liquid pipeline transmission companies. The American Petroleum Institute (API) represents more than 470 oil and natural gas companies, leaders of a technology-driven industry that supplies most of America's energy, supports more than 9.2 million U.S. jobs, accounts for 7.7 percent of the U.S. economy, and delivers more than $85 million a day in revenue to the U.S. Treasury. Together, our organizations represent the operators of approximately 90 percent of total U.S. oil pipeline mileage in the United States.

Pipelines are the safest, most reliable, economical, and environmentally favorable way to transport oil and petroleum products, other energy liquids, and chemicals throughout our Nation.

Liquid pipelines bring crude oil to the Nation's refineries and petroleum products to our communities, including all grades of gasoline, diesel, jet fuel, home heating oil, kerosene, and propane. AOPL's and API's member companies provide hydrocarbon feedstocks for use by many other industries, including food, pharmaceuticals, plastics, chemicals, and road construction. America relies on the network of more than 170,000 miles of liquid pipelines to move the energy that fuels our Nation's economic engine and delivers the products to keep our Nation's industry in operation. Colonial as a company, and the pipeline industry as a whole, are committed to delivering these materials safely and efficiently.

I am pleased to have the opportunity to provide some perspective on behalf of the liquid pipeline industry as the subcommittee conducts its important oversight of the reauthorization of the Transportation Security Administration (TSA).

PIPELINE OPERATORS INSIST ON SAFETY

Pipeline operators have every incentive to invest in safety. Indeed, in our members' view, there are no incentives to cut corners on pipeline safety. Most important is the potential for injury or loss of life to members of the public, pipeline employees and contractors. As an industry we also recognize the impact we could have on the environment and to our country's economy. In addition to the public and third-party impact, if a pipeline experiences a failure or a release, there are numerous potentially harmful consequences for the operator and its reputation. The operator could face litigation, fines, incur potentially costly repairs and cleanup costs. Further, the pipeline could suffer a significant loss of revenue and goodwill by not being able to serve its customers for extended periods of time. In short, when it comes to safety, pipeline operators have every reason to operate in a manner consistent with the public interest.

Pipeline operators invest millions of dollars annually to maintain their assets and comply with Federal safety laws and regulations. A large percentage of liquid pipeline assets are inspected regularly and all are monitored continuously. Safety measures include proper pipeline route selection, design, construction, operation, and maintenance, as well as comprehensive public awareness and excavation damage prevention programs.

Pipeline safety is closely regulated by the Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA). PHMSA is responsible for establishing and enforcing regulations to assure the safety of pipelines (Title 49 CFR Parts 190–199). Operators face a rigorous set of PHMSA regulations pertaining to pipeline construction, operation, and maintenance. Regulations also cover public awareness, reporting, design standards, construction methods, operational controls and limitations, pressure testing, maintenance standards, qualification of personnel, and emergency response. These same laws and regulations also address the leading causes of pipeline failures, including corrosion, excavation damage, materials and equipment failure, and operational errors.

PIPELINE SECURITY—OVERVIEW

With regard to the security of the pipeline industry, the private and public sectors share the same goal: To protect our facilities from attack so that we can avoid loss of life, disruption of service, damage to our assets, injury to our employees and the public, and harm to the environment and the economy. We must, however, also recognize that our sectors share the same limitation: We must allocate resources

through a risk-based approach that properly assesses the likelihood and consequence of an event at a facility.

I cannot stress enough that the key to effectively managing this risk requires what TSA has properly called a "partnership" between the private and public sectors. The success of this and any "partnership" is dependent upon communication and collaboration between the parties. In my view, the most effective security program will be one that is not static, but rather constantly changes and improves to ensure that we are staying ahead of increasingly sophisticated adversaries that would do us harm. Regular interaction with TSA through a strong partnership ensures that we are evolving at the greatest speed possible by taking advantage of the knowledge and strengths that each sector can provide.

Prior to the tragic events of September 11, 2001, pipeline safety and security were both under the jurisdiction of what is now PHMSA's Office of Pipeline Safety (OPS). On November 19, 2001, President George W. Bush signed the Aviation and Transportation Security ACT (ATSA) establishing TSA and designated it as the lead Federal agency for transportation security including pipelines. Following these events, the Department of Homeland Security (DHS) was created on November 25, 2002, transferring TSA into the newly created DHS. Federal guidance was published by OPS on September 5, 2002, through a circular notice that recommended pipeline operators identify critical facilities, develop security plans, an implementation schedule for these plans, and the need to review them annually. On December 17, 2003, President Bush issued Homeland Security Presidential Directive—7 (HSPD–7) that required DHS and other Federal agencies to collaborate with appropriate private sector entities to assist in the protection of National critical infrastructure. Further, representatives of DHS and DOT signed a Memorandum of Understanding (MOU) in September of 2004, which reiterated DHS's jurisdiction for the security of all modes of transportation. In essence, the role of PHMSA's oversight is related to the safe operation, construction, and maintenance of pipelines, and PSD is responsible for ensuring that pipeline facilities are adequately secure from security-related threats.

PSD is located within the Office of Transportation Sector Network Management (TSNM) and has been directed to enhance the security preparedness of the Nation's liquid and natural gas pipeline systems by:

- Developing security programs and conducting analysis to maintain pipeline and domain awareness with particular focus on critical systems and infrastructure;
- Identifying industry best practices and lessons learned; and,
- Maintaining a dynamic modal network through effective communications with the pipeline industry and Government stakeholders.

PSD ACTIVITY

Following the direction of HSPD–7, PSD developed a comprehensive security program that is predicated on the agency's interaction with the pipeline industry.

PSD regularly conducts Corporate Security Reviews (CSR) of major pipeline operators to assess their security plans and implementation. As the PSD staff conducts on-site reviews, the CSRs also help to establish working relationships with key security representatives in the pipeline industry.

To date, PSD has conducted 115 CSRs of the largest operators in the United States, and it has also conducted Critical Facility Inspections (CFI) of the most sensitive locations in the pipeline industry. The CFIs are in-depth reviews that focus on the implementation of security plans and actual practices at critical facilities. The results of these reviews have been used to develop security "smart practices" that can be shared across the industry. According to the PSD, they completed CFIs of all identified locations earlier this year.

PSD has also promoted the use of the Transportation Security Operations Center (TSOC) as a point of contact for pipeline operators to report any significant security incidents or suspicious activities. The TSOC is staffed 24 hours per day and disseminates the information it receives to the appropriate agency or division for response.

In May 2007, TSA issued the *Transportation Systems Sector Specific Plan and Pipeline Modal Annex* that is part of the *National Infrastructure Protection Plan.* The Pipeline Modal Annex has many items, including: A description of risk-based security programs, security program management, and site and program assessment.

Most recently, PSD completed more detailed and specific Pipeline Security Guidelines in December 2010. The pipeline industry has worked with PSD for several years in the development of the Pipeline Modal Annex and generally supports the recently issued Pipeline Security Guidelines. TSA built on the previous guidance

issued in 2002 and the requirements of the 9/11 Commission Act of 2007 to provide specific Federal recommendations for pipeline safety security practices.

TSA AND INDUSTRY

Communicating and coordinating with stakeholders enables the public sector to have an uninhibited view of the pipeline industry's approach to security. With this enhanced perspective, PSD not only gains a clear and accurate view of the industry's capabilities, but is also able to identify any gaps that may exist. The private sector benefits from this collaboration because any potential shortfalls identified by PSD can quickly and effectively be communicated to the industry and acted on immediately. Again, the goal of providing appropriate security for the pipeline industry as a component of our Nation's critical infrastructure is one that is shared.

Overall, PSD has assumed a responsible approach to pipeline security. PSD has worked with other agencies, including DOT and the Department of Energy (DOE), and with industry, through the Oil and Natural Gas Sector Coordinating Council (ONG SCC) and the Pipeline Sector Coordinating Council (Pipeline SCC), to identify effective and practical security practices for pipeline operators.

In accordance with the National Infrastructure Protection Plan (NIPP), a Critical Infrastructure Partnership Advisory Council (CIPAC) Oil and Natural Gas (ONG) Joint Sector Committee was established to provide a legal framework for members of the Energy and Transportation Sector GCC and ONG SCC to engage in joint critical infrastructure protection discussions and activities, including those involved with pipeline security. Nineteen industry trade associations came together to form the ONG SCC to help facilitate communications between industry security professionals and representatives of the Energy Sector Government Coordinating Council. Soon after, the Pipeline Working Group (Pipeline Sector Coordinating Council) was formed to further improve communication and collaboration among pipeline operators and various Government agencies.

The ONG SCC provides a forum for industry to discuss relevant security issues and coordinate and communicate with agency counterparts. Quarterly meetings are held with SCC representatives and also jointly with members of the Government Coordinating Council (GCC). The ONG SCC serves as a point of coordination for broad communication with the security representatives of the oil and natural gas industry as well as partners in State and Federal Government. Members of the ONG SCC provided significant input to TSA during the development of the *Transportation Sector Specific (Security) Plan* that was included as part of the *National Infrastructure Protection Plan* process.

The ONG SCC has several different working groups that specialize in key security areas, such as Information Sharing—Homeland Security Information Network, Cyber Security, and Pipeline Security. The Pipeline Working Group includes representatives of industry operators and four of its major trade associations: AOPL, API, the American Gas Association (AGA), and the Interstate Natural Gas Association of America (INGAA). The Pipeline Sector Coordinating Council also meets periodically with its counterparts in the Pipeline Government Coordinating Council, which is chaired by a representative of PSD and includes representatives of DOT and other Federal agencies. Members of the Pipeline Working Group have provided substantial input to TSA PSD to assist in its development of the 2010 Pipeline Security Guidelines. The Pipeline SCC and GCC have proven to be positive venues to improve communications between industry and the agencies.

PSD also interfaces with industry by providing important services and tools, such as Pipeline Security Training videos, conferences, and forums to share information and experiences to improve security at our Nation's critical infrastructure. For example, TSA conducts an annual International Pipeline Security Forum in partnership with Natural Resources Canada that brings together pipeline security professionals and representatives of other appropriate Federal agencies that have a nexus. These programs have not only provided a means of evaluating the actual security practices of the pipeline operators, but have also been a means of promoting industry familiarity with the responsibilities and personnel of the PSD.

AREAS OF SUGGESTED IMPROVEMENT

As I have mentioned above, the pipeline industry has a constructive working relationship with PSD. In light of the oversight role today's hearing will play in the reauthorization of TSA, it is important to highlight a few areas of concern. Rarely will industry and regulators agree on every point or proposal, however, we believe there are some issues that could be resolved at DHS with improved communication and reasoned decision-making.

For instance, this subcommittee is well aware of the need and importance of the Chemical Facilities Anti-Terrorism Standards, also known as CFATS. Section 550 of the Homeland Security Appropriations Act of 2007 required DHS to establish risk-based security standards for chemical facilities. Contrary to initial indications from DHS, CFATS regulations were expanded to include operators of gasoline storage facilities by the incorporation of a "flammable mixtures" provision late in the regulatory development process. AOPL, API, and the National Petrochemical and Refiners Association (NPRA) filed joint comments asking DHS to review the technical deficiencies of its rulemaking, and industry suggested the creation of a technical panel comprised of independent experts to assist the agency in making its tiering decisions. For over 2 years, industry has awaited a formal reply from DHS in response to what we believe to be very legitimate scientific concerns about how CFATS risk decisions were determined with respect to flammable mixtures in above-ground storage tanks.

Another, and less technical, example at DHS is the issue of proposed redundant background checks through proposals such as the Personnel Surety Program (PSP). The liquid pipeline industry and others within the Oil and Natural Gas Sector support strong and effective risk-based security standards of high-risk facilities in order to ensure safeguards are in place to protect critical infrastructure. Our industry supports credentialing programs that can efficiently and seamlessly check Personally Identifiable Information (PII) against the Terrorist Screening Database (TSDB). However, we are concerned that DHS's proposal would create significant new administrative burdens by making personnel vetting applicable to facilities rather than individuals, with no enhancement to security. Rather than creating a redundant PSP to be administered by the Chemical Compliance Division, it would be more logical for DHS to leverage the existing Transportation Worker Identification Credential (TWIC) program to provide personnel security clearances at chemical facilities. The TWIC program is already administered by TSA and the U.S. Coast Guard, and is widely accepted and utilized in the pipeline industry. Making specific enhancements to the existing, in-place TWIC program as opposed to initiating what appears to be a redundant and duplicative PSP effort is a more logical approach. Despite the many talented and well-intentioned individuals within DHS, this general lack of transparency in their decision-making process hampers productive dialogue between Government and industry, and ultimately, threatens to errantly commit precious resources needed to help ensure a secure National infrastructure. I want to thank this subcommittee and its Members for addressing this issue in your recent mark-up of HR 901. It is our hope that this proposal will be a part of a final CFATS reauthorization bill this year.

In closing, thank you again for the opportunity to appear before you today and share my views and can personally attest to the productive working relations the pipeline industry has with PSD. I would be happy to answer any questions that you may have.

Mr. ROGERS. Thank you, Mr. Reese, for your testimony. As I pointed out a little while ago, your pipeline runs through my district, so I really like it.

Our fifth witness Mr. John Risch. He is the alternate National legislative director for the United Transportation Union.

The Chairman now recognizes Mr. Risch for your testimony.

STATEMENT OF JOHN RISCH, III, ALTERNATE NATIONAL LEGISLATIVE DIRECTOR, UNITED TRANSPORTATION UNION

Mr. RISCH. Chairman Rogers, Ranking Member Jackson Lee, Members of the committee, on behalf of the 85,000 members of the United Transportation Union, I would like to thank you for the opportunity to address this committee today.

UTU represents thousands of transit and rail employees. Each and every day, our members are on the front lines of the battle to keep our transportation network secure. Our members are committed to work with their employers and our Government to improve our lines of defense against those who wish our Nation harm. UTU has offered to work with our Nation's railroads on security

training and has had positive discussions on possible joint partnerships.

A primary concern to our rail members is the lack of locks for doors and windows on locomotive cabs. We believe it should be a requirement that all locomotives be equipped with locks for the doors and windows to prevent unauthorized entry into the operating compartment. When windows and doors are closed and locked, the locomotive cab needs to be air-conditioned. Certainly, in cold weather, operating crews will close the windows and doors. However, in hot weather, without air-conditioning, operating crews are forced to open the doors and windows, compromising their personal safety and that of others.

Currently, there is no Federal standards for equipping locomotives with air-conditioning or for secure locks on doors and windows. But we are pleased to say that the Federal Railroad Administration is currently developing regulations that address the issue of air-conditioning, but not on locks and doors.

I would like to clarify, in my written statement I did mention a terrible incident that happened in New Orleans last year. I have now been told by the railroad involved that the cab did have locks on the windows and that particular locomotive cab did have air-conditioning.

In regards to our bus members, operations in the bus industry, we recommend that bus terminals be secured with fencing, video cameras, security personnel, or a combination of all three. Many bus yards are not fenced, and many that are do not have locked gates.

In regards to security training for employees, we need to adequately train hundreds of thousands of transit and rail workers across America so that they are ready in the event of a terrorist threat or attack. In emergency situations, our members are the first on the scene, even before police, firefighters, and emergency medical responders, and what they do in the first few minutes is crucial to minimizing destruction and loss of life. These employees need to know how to recognize a potential problem, what protocols to follow for reporting and responding to potential threats, and how to protect themselves and others from harm.

This committee worked diligently to address these concerns by including comprehensive training in the 9/11 Commission Act. That legislation mandated that all front-line transit, rail, and over-the-road bus employees undergo live training exercises, receive training on evacuation procedures, and be instructed on crew and passenger communications and coordination.

Unfortunately, these training mandates are nearly 4 years overdue. In fact, this administration has failed to issue a notice of proposed rulemaking on these essential training issues. We believe this is unacceptable, and further delay only perpetuates the existing dangers.

I worked as a locomotive engineer for 30 years on a large freight railroad. In my entire career, my security training consisted of watching a 30-minute video in a cubicle by myself. The video was well-done, and it urged me to report any suspicious activities and how to be more aware of my surroundings. However, it was not tailored to my job responsibilities, and I didn't learn any specific

skills. That video, while a good tool, did not constitute meaningful training.

In our industry, training in general has evolved away from the classroom and into the cubicle. Where we once had discussions with coworkers and instructors, we now have hours in front of computer screens with no opportunity to interact and ask questions. It is tantamount to training on your own. We need legitimate classroom training using security professionals. Security training should also be redundant and not a one-time, check-the-box exercise for employers.

In closing, workers must be treated as partners in the battle to protect our vulnerable rail and public transit systems, and, through proper training, they will be prepared to do so. We appreciate this committee's efforts to push for meaningful security initiatives. We strongly urge TSA to implement the training mandated in the 9/11 Act to ensure front-line workers are prepared to assist in the event of an emergency.

Thanks again for the opportunity to appear.

[The statement of Mr. Risch follows:]

PREPARED STATEMENT OF JOHN RISCH, III

JULY 12, 2011

Chairman Rogers, Ranking Member Jackson Lee, and Members of the subcommittee, on behalf of the 85,000 members of the United Transportation Union (UTU) thank you for the opportunity to testify today at this important hearing on transportation security.

UTU represents thousands of transit and rail employees on our Nation's freight and passenger rail systems, including Amtrak. Each and every day these workers are on the front lines of the battle to keep our transportation networks secure. Our members are committed to work with their employers and our Government to improve our lines of defense against those who wish our Nation harm. UTU has offered to work with our Nation's railroads on security training and have had positive discussions on possible joint partnerships.

A primary concern to our rail members is the lack of locks for doors and windows on locomotive cabs. On June 20, 2010, in New Orleans a conductor was shot to death and the locomotive engineer was injured during an armed invasion and robbery in their locomotive cab. The lack of a secure operating cab allowed that individual to easily enter the cab and commit this terrible crime. Also in 1998 a commuter train was hijacked when an intruder entered the unlocked locomotive cab. The locomotive engineer was held at gunpoint and the train was hijacked to Philadelphia. We believe it should be a requirement that all locomotives be equipped with locks for the doors and windows to prevent unauthorized entry into the operating compartment.

When windows and doors are closed and locked, the locomotive cab needs to be air conditioned. Certainly in cold weather operating crews will close the windows and doors; however, in hot weather without air conditioning, operating crews are forced to open the windows and doors, compromising their personal safety and that of others.

Currently there are no Federal standards for equipping locomotives with air conditioning or for secure locks on doors and windows. We are pleased that the Federal Railroad Administration (FRA) is considering the issue of air conditioning in a pending rulemaking, but unfortunately requiring locomotive doors and windows to have locks is not part of that rulemaking.

In regards to bus operations, we recommend that bus terminals be secured with fencing, video surveillance, security personnel or a combination of all three. Many bus yards are not fenced and many that are do not have locked gates.

In regards to security training for employees, we need to adequately train hundreds of thousands of transit and rail workers across America so they are ready in the event of a terrorist threat or attack. Properly training frontline workers is vital to surface transportation security and is a cost-effective way to secure and safeguard our transit and rail networks.

In the event of an incident or attack, our members are the first on the scene—even before police, fire fighters, and emergency medical responders—and what they do in the first few minutes is crucial to minimizing destruction and loss of life. On the transit and passenger rail side, workers are often called upon to evacuate passengers away from an incident. On freight railroads, workers are needed to help mitigate damage to facilities and equipment and alert first responders. These employees need to know how to recognize a potential problem, what protocols to follow for reporting and responding to potential threats, and how to protect themselves and others from harm.

Officials from the Federal Transit Administration (FTA) and the Transportation Security Administration (TSA) have testified before Congress on the need for, and the inherent value of, worker security training. Yet too little has been done to actually ensure that employees receive adequate security training because railroads and transit systems are not currently required to provide adequate training.

This committee worked diligently to address these concerns by including comprehensive security training in the 9/11 Commission Act. That legislation mandated that all front-line rail, transit, and over-the-road bus employees undergo live training exercises, receive training on evacuation procedures, and are instructed on crew and passenger communications and coordination. Unfortunately, these training mandates are nearly 4 years overdue. In fact, this administration has failed to issue a Notice of Proposed Rulemaking (NPRM) on these essential training issues. We believe this is unacceptable and further delay only perpetuates the existing dangers.

In many cases security training consists of a pamphlet or a short video. I worked as a railroad engineer on a large freight railroad for 30 years and my entire security training consisted of watching a 30-minute video in a cubical by myself. The video was well done and it urged me to report any suspicious activities and to be more aware of my surroundings. However, it was not tailored to my job responsibilities and I didn't learn any specific skills—I was simply instructed to be more vigilant. That video, while a good tool, did not constitute meaningful training.

In the railroad industry there are enormous amounts of operational testing that takes place, where supervisors spy on workers hoping to catch someone committing some petty infraction of the rules. We have had supervisors sneak around in camouflage clothing, use unusual vehicles and use other means to disguise their identity. Many of my co-workers didn't report suspicious activities because they believed that the person sneaking around was probably a supervisor.

Another concern to us is the way in which training in general has evolved away from the classroom and into the cubical. Where we once had discussions with instructors and co-workers, we now have hours in front of computer screens with no opportunity to interact and ask questions. This is tantamount to "training on your own." We need legitimate classroom training, using security professionals. While videos and computer-based training can be supplements, they are not a meaningful substitute for classroom training. Workers need the opportunity to ask questions about their particular workplaces and need training that is designed to fit their craft and work environment.

Security training should also be redundant, not be a one-time, check-the-box exercise for employers. Workers cannot be expected to retain and apply skills that they were exposed to only once. Regularly scheduled follow-up training is critical to make sure workers are effective on our Nation's front lines.

Some additional recommendations are:

- The security of major rail terminals where chemicals are stored requires increased protection whether by additional fencing, video surveillance, security personnel, or a combination all these tactics.
- We recommend additional track inspections to verify the integrity of the right of way as a cost-effective way in which to protect our rail system.
- We believe that the current FRA regulation on glazing standards provides an insufficient level of protection for crew members. Those standards require locomotive glass to withstand the ballistic impact of a .22 caliber lead bullet of 40 grains. This standard has been in effect for decades and is outdated. Most firearms far exceed this level of protection. While there are firearms that can penetrate almost any glass thickness, we don't believe that is a legitimate reason to do nothing. If a glazing is available that can protect operating employees from most of the firearms available to today, then Congress should require the installation of such glazing on locomotives.

In closing, workers must be treated as partners in the battle to protect our vulnerable rail and public transit systems, and through proper training they will be prepared to do so.

We appreciate this committee's efforts to push for meaningful security initiatives. We strongly urge TSA to implement the training mandated in the 9/11 Act to ensure

front-line workers are prepared to assist in the event of a transportation security incident.

Thank you for the opportunity to share the United Transportation Union's views.

Mr. ROGERS. Thank you for that testimony.

I thank all the witnesses.

We will start with questions now, and I will lead off.

I want to follow up on that point right there, because I met with Chief Dunham before the hearing, and she talked about the extensive training that her transit employees undergo.

Is it automated like that? Describe what your training is for your transit security individuals.

Chief DUNHAM. Yes, sir. As we spoke earlier, we were talking about the fact that you have to train every employee. I think as we were talking about with the airlines, the flight attendants, everyone, whoever is going to be the first person there. So you have to train everyone, not just specialized teams of people, but you have to train everybody. So we make sure that every one of our employees is trained on any active shooter——

Mr. ROGERS. Is it just watching videos, or do they train——

Chief DUNHAM. Oh, no, no. There is live instruction. It is a layered approach. So there is live instruction. There is hands-on, because I think we learn from hands-on, as well. So it is a lot of participation—a lot of participation in whatever the training is.

So, I think it—and the good thing about it is that all the training is grant-funded.

Mr. ROGERS. Right.

Mr. Risch, you talked about, all you had was a video to watch. Do you still see that occurring in any of the transportation modes that we are talking about here today?

Mr. RISCH. Well, I only represent the bus and the rail industry. It varies from railroad to railroad, bus company to bus company. It is not uniform. Currently, there is nothing requiring the length and type of training that is going on.

The Federal Railroad Administration is actually adopting some regulations on training standards, but they only apply to operational rules in Federal regulations. They don't apply to security training. Through that process, we have urged more comprehensive hands-on training.

Mr. ROGERS. Well, that is why I wanted to visit that, because my interaction with all the various transportation sectors has led me to believe that the training is, today, more detailed than having people watch a video. If that is prevalent, you know, we want to know about it so we can work to change that fact.

I want to go to Mr. Farmer.

You talked in your opening statement about the need for better intelligence sharing, and you have told me that months ago in a private meeting. Are you seeing any improvements? If so, or even if not, what can we do in the reauthorization that would facilitate better communication to and from TSA to the rail industry?

Mr. FARMER. Sir, we are seeing improvement in at least a willingness to discuss changes in approach.

We have presented our intelligence requirement to a number of entities: TSA's Office of Intelligence, DHS's Office of Infrastructure Protection. We even had a chance to participate in a stakeholder

outreach program with the Office of the Director of National Intelligence.

The problem is, there was a lot of nodding of heads that it is a good idea, this focus on the preparatory aspects of terrorist operations, but there does not seem to be a willingness to make the necessary adjustments in priorities for any one of those entities to take that on.

Mr. ROGERS. Well, and that is what I am asking. Is there something that you would like to see in the reauthorization language that would set that framework so that you would have a higher degree of confidence in this necessary back-and-forth of information?

Mr. FARMER. I think what the authorization act could discuss, in particular, are two areas: A rail security strategy—let's boil this down to some fundamental priorities.

One of the best documents you can read is National Security Decision Directive 75. It was put out by the Reagan administration in 1983. It is now declassified. It was the strategy that won the Cold War. It is 8 pages long.

Mr. ROGERS. Uh-huh.

Mr. FARMER. Most of what you see coming from the Federal Government is in the dozens to hundreds of pages in length. So that is one area; let's talk about some very core, fundamental priorities that we can measure each other against.

On the issue of information sharing, there is a lot of volume shared but, often, it is after the fact. We are told that on a certain date at a certain time an event happened, it involved this type of explosive, and there were this many casualties. What we are not getting is an analysis of, well, what happened on the beforehand?

So, really, what we are looking for is some entity in the Federal Government—and I think TSA is the best place to do this, with its Office of Intelligence—to do that analysis, to become for the Federal Government the resource for transportation-related security intelligence.

DHS has an excellent tool; it is a diagram that shows the various steps of the terrorism planning cycle. But what we have never seen is someone break down an operation or a composite of operations against that cycle. Then we can look at it and see where opportunities for security existed that could have made a difference.

So in terms of an authorization, setting as a priority for preparing security professionals in railroads, in transit agencies, in trucking, to understand the nature of the adversary they face by knowing what we can know. These attacks have happened. They have happened overseas. We have had disrupted plots here. We are not drawing enough from what can know about how this is done.

Mr. ROGERS. Excellent.

My time is up, and I look forward to asking some more questions in our second round.

The Chairman now recognizes the Ranking Member for any questions she may have.

Ms. JACKSON LEE. Thank you, Mr. Chairman.

I have so many, and I am going to ask as many as I can. I would ask you to help me with your answers so that I can ask all of you questions based on some very, very important testimony.

The continuing theme that I heard is we need training, training, training, and we need access to information to help us be able to interpret the threat that is around us. I thank you for that, and I think that is going to be very important as we move toward an authorization bill.

If I might ask Mr. Risch specifically, I have the privilege of representing Houston, Texas, that has as its insignia or its motto—insignia, let me say—is a railroad as the symbol of our city. That means that we have rail lines through residential neighborhoods and near schools and a lot of facilities where people are ingressing and egressing.

Tell me, if you could create a training program for this environment, what types of things would you focus on?

Mr. RISCH. Well, certainly, you need to train people to be vigilant and watch out for suspicious activity and a real opportunity to report those to the right people so action can be taken.

I think what you need is a classroom environment, where an instructor is there, where the individual workers can interact with the instructor and their co-workers saying, well, you know, discuss things like there may be places where chemical cars are parked or routinely stored, that you have to be very diligent in those types of areas.

There would be a host of things—I think people that are trained in security and know what to look for would be the appropriate ones to do the training, not some——

Ms. JACKSON LEE. Video.

Mr. RISCH [continuing]. Railroad guy or video that really doesn't understand the potential threats.

Ms. JACKSON LEE. So we need hands-on training.

Mr. RISCH. That is correct.

Ms. JACKSON LEE. Mr. Reese, working with the pipelines certainly is very familiar in the State of Texas. You had an incident that just occurred in Montana. The potential for terrorist threats against pipelines, I think, is great.

What specifically can we do to add to the securing of pipelines, training and otherwise?

Mr. REESE. That is a great question, ma'am.

What I see going on right now with TSA is a lot like what I have heard elsewhere: The default is a video, because it leverages so much in such an efficient manner. I am not necessarily opposed to video as a platform for training. I think more importantly is knowledge transfer. So if there is some kind of confirmation process to ensure that the instructor is qualified and that the individuals who sat in on the training actually understand the mission, I think video can be incorporated in an overall training program.

What TSA chooses to do is provide video that is targeted for both law enforcement and operators, which I think is effective because the interests are slightly different, the needs for information are slightly different, but they both need to have training.

I also see more in-depth training being offered that would be, by default, reserved for the Government, the public side of the house, but that is extended to the private side based on positions and so forth inside companies, where there are security experts and so forth. That is helpful. There are also forums and the clearance

process that allows people in industry to have access to classified information on a need-to-know basis.

Ms. JACKSON LEE. Maybe I will come back to you, because I wanted to focus on what you can do to secure your pipelines. But let me quickly ask—and I appreciate that answer.

Let me quickly ask the chief, Mr. Rojas, and Mr. Farmer:

Chief, what would happen to you with the underfunding of the Transportation Security Grant Program?

Mr. Rojas, could you re-emphasize the importance of streamlining TWIC, making it the single security document, in helping us with security?

Mr. Farmer, can you tell us how we can harmonize TSA's rail security standards and expectations with the issues and concerns you have with the American Railroad Association?

Let me go to the chief first, please. Thank you.

Chief DUNHAM. Yes, ma'am, thank you. That is a great question.

In the State of Georgia, we are one of the only transit agencies to not really receive any grant funding—or, any kind of subsidies from the State of Georgia. So grant funding is the only thing that we have in order to target harden our system. So, without that funding, you know, we would be left susceptible to any kind of terrorist threats.

So it is very important for us, and that is why we really need to continue this program and get more allocations. Because we are considered a Tier 1 agency, which means that, you know, a terrorist attack is likely to occur in our city. So we definitely would need that funding.

Ms. JACKSON LEE. We thank you.

Mr. Rojas.

Mr. ROJAS. Thank you. We believe——

Ms. JACKSON LEE. Microphone.

Mr. ROJAS. Sorry.

We believe the TWIC credential can certainly function as an excellent both security threat assessment and an access credential for multiple facilities. As I explained in my comments, the issue is that we enter so many different types of facilities, from maritime to rail yards. As Mr. Reese explained in his comments—and that was not purposely done so—was the fact that there are so many areas that we have to gain access to, that if each one of these different facilities required a separate credential and a separate access card per se and a separate background check potentially, we would find ourselves wearing too many credentials and having to undergo too many background checks.

So I think we can arrive at a point where we have a single process and a single system. We recognize that we have to make the credentialing process better, and I think TSA is aware of that, too. So we are very supportive of the TWIC concept.

Ms. JACKSON LEE. Mr. Farmer, quickly on my question. Thank you.

Mr. FARMER. Yes, ma'am.

The challenge that the railroads face, because they operate across many States, and particularly the Class I railroads and Amtrak, is that, because the TSA surface inspectors are supervised locally, the priorities they pursue, the interpretations of the regula-

tions that they bring to bear, can vary significantly from place to place.

So we have had situations where railroads are taking actions that are seen as compliant by some TSA officers in the field and yet are treated as violations by others. We believe some form of oversight from the headquarters level or through these regional security inspectors that I referenced would be a way to overcome that problem.

I will give you a very practical example of what happens. The last statistic I heard, at a meeting we had with TSA in March in Fort Worth, was that the agency had issued 17 letters of investigation alleging potential violations of TSA security regulations. Seven of those had to be withdrawn by TSA headquarters because they simply did not state a meritorious case. Yet when those letters show up at the railroad, they are talking about fines measured at $10,000 per violation. Of the remaining 10, none actually alleged any sort of noncompliance with a substantive security issue at hand. They were alleging errors in documentation.

The concern, again, is that, when these standards vary, you have a situation where 40 percent of the letters of investigation sent to railroads are kicked out because they are simply not meritorious. Better coordination between the headquarters, where the inspectors are following the headquarters' priorities, can bring that consistency, so a railroad, Class I freight railroad, Amtrak, can rely upon a similar interpretation of a rule wherever it operates.

Ms. JACKSON LEE. Thank you.

Mr. Chairman, on his point, I just can't imagine not having consistent inspectors—which my legislation, H.R. 19, tries to address—well-trained Federal inspectors that are consistent all over America when they inspect these railroads.

Let me thank the witnesses.

Thank you for your indulgence, Mr. Chairman. I yield back.

Mr. ROGERS. I thank the gentlelady.

The Chairman now recognize the gentleman from Minnesota, Mr. Cravaack, for 5 minutes.

Mr. CRAVAACK. Thank you, Mr. Chairman. I appreciate it.

Thank you very much for being here today.

A real quick question. I understand that, from 2008 to 2011, we have gone from 175 inspectors to 380 inspectors.

In your opinion, Mr. Farmer, do you think that that has increased the security of your system while, at the same time, maybe the inconsistencies you were just speaking of are because of the rapid deployment of the security force? What is your opinion?

Mr. FARMER. The rapid increase of the force—and I think now it is actually over 400, is the most recent statistic that I heard. The rapid increase of the force has caused a departure from what was the fundamental premise of the hiring of those inspectors at the outset of the program back in 2005–2006. There was very much then a focus on hiring people with a rail background, a transit background. One of the concerns now is that they are not getting those people into these positions. They don't have extensive rail or transit experience. They are not bringing to bear a familiarity with the environment.

That does create safety concerns, since, often, railroads are the entities that are orienting the inspectors to the dangers in the environment. But, more importantly, the lack of familiarity with rail generally does create a situation where these sorts of inconsistencies become more likely, especially if there seems to be a disconnect, often, between what priorities are set at the headquarters and what gets executed in the field.

Mr. CRAVAACK. Mr. Rojas, do you feel the same way?

Mr. ROJAS. The issue for us has to do with, obviously, we have a much larger population of trucking companies out in the field, with about 600,000 trucking companies registered with the U.S. Department of Transportation for interstate commerce and another 500,000 registered for intrastate commerce.

So we need to have some level of harmonization in that area. I think it would be important, because we have had some issues where inspectors have come up, some of the VIPR teams actually, we have had some issues with VIPR teams asking truck drivers if they actually have a TWIC, for example, and for no specific reason. They might not be near a port.

So we have some issues in this area, and we certainly, you know, look forward to working with TSA and the committee on this issue.

Mr. CRAVAACK. So you probably think that training of the inspectors themselves is the issue?

Mr. ROJAS. Well, the problem is that we deal with a lot of different law enforcement agencies. If you think about it, the commercial vehicle inspectors are State troopers. We obviously deal with different—on the highways, we deal with a number of different law enforcement agencies. I think there is a concern by the drivers sometimes, in dealing with too many law enforcement people, you know, there is a sense that it is a bit overwhelming for the drivers in how many law enforcement agencies we have to deal with.

So, all of a sudden, they have one more inspector asking them for yet another credential or another training component or something like that. It gets a little overwhelming for the truck drivers.

Mr. CRAVAACK. While they are trying to get their freight delivered on time.

Mr. ROJAS. That is correct.

Mr. CRAVAACK. Chief Dunham, could you expound, ma'am?

Chief DUNHAM. Yes, sir. Thank you.

One thing to keep in mind is that the increase in security inspectors does not mean more security. I think people get confused by that. They are kind of an oversight. Sometimes it is a little bit much for them to come in, like Mr. Rojas said, yet another inspector to come in. I need more boots on the ground. I need more people in the field.

Mr. CRAVAACK. Thank you, ma'am.

Mr. Reese, would you care to comment, sir.

Mr. REESE. I would echo Mr. Rojas' comments concerning harmonization. I don't know that it is as much a training issue as it is a standardization issue. If the collective inspectors interpret their regs the same way, approach the work the same way, then you get a more consistent application of the inspection process. I will hold it there.

Mr. CRAVAACK. Thank you, sir.

Mr. Farmer, I am very fortunate to have International Falls, Minnesota, in part of my district, which is a big rail point for border security.

Can you tell me a little bit about the TSA's rail security inspection activities at points such as that, which has a lot of rail go through it? I was wondering if you could expound upon that a little bit?

Mr. FARMER. Well, I think, sir, in areas like that, you would have inspections from the two DHS components, the TSA surface inspectors, looking to any issues involving the various action items they oversee or regulations, particularly pertaining to transport of hazardous material. Obviously, you also have potential interest from Customs and Border Protection looking at issues there as commerce goes back and forth across the border.

The railroads spend an awful lot of time and effort in cooperation with both CBP and TSA in this area. In particular, with Customs and Border Protection, there are joint working groups that focus specifically on enhancing cross-border security. Some of our railroads actually operate across border, and particularly on the northern border, Canadian National and Canadian Pacific.

Each of those railroads has their own rail police departments. When the traffic crosses the border, when it goes through the Customs and Border Protection checkpoint, there is a screening system that evaluates those cars to look for any indications of contraband.

So it is a good collective and extensive effort where significant attention is paid both by the rail industry and the Government to try to mitigate and minimize the use of a train as a means to get something illicit into the country.

Mr. CRAVAACK. I have been up there to see those teams. They are great teams up there.

With that, sir, I will yield back.

Mr. ROGERS. I thank the gentleman.

The Chairman now recognizes the gentleman from Michigan, Mr. Clarke, for any—all right. Well, then we will go back to the Chairman.

One of the things that I wanted to visit—and I have talked with most of you about this privately—is, do you see any rules and regulations that are still hanging out there that really need to be pruned back that are no longer relevant or applicable or are duplicitous?

Let's start with Mr. Rojas on that.

Mr. ROJAS. Thank you, Mr. Chairman.

I think the Obama administration actually issued an Executive Order, 13563, in relation to this very issue of overlapping regulations, and we certainly submitted comments. Obviously, for us, the major one, the first one is the credentialing, as you well know.

Some of the other issues that we have been dealing with relate to some of the validation process of some of the audits or visits that multiple agencies do sometimes. I know TSA has been developing a corporate security review. At the same time, the U.S. Department of Transportation has been doing security compliance reviews. It just seems to us that there should be an ability to coordinate and communicate a little closely as to what the results of each are so we don't get multiple visits per se.

At the same time, many of our carriers are also members of the Customs-Trade Partnership Against Terrorism, and they have undergone validations for C–TPATs. So the number of programs out there is certainly a concern to our industry, in that sense.

Mr. ROGERS. Excellent.

Mr. Farmer.

Mr. FARMER. In the area of security, one of the challenges that you run into is overlap, at times, between regulations maintained by the Department of Transportation and then those subsequently put in place by TSA—or, to be put in place by TSA. There was reference earlier to the rulemakings under the 9/11 Act for training, and there is also one that pertains to security plans.

Specifically with TSA, the predominant regulation that has an effect on the railroads is 49 CFR part 1580. It focuses on reporting of security concerns, appointment of a security coordinator, and, in particular for freight railroads, specific requirements that pertain to the transport of toxic inhalation hazardous materials.

We do believe that those regulations, now in effect for a couple of years—the process to develop them started 5-plus years ago—that there is an opportunity to look at some of the specific processes under those rules to determine whether they are necessary at this point.

In the area of training, the railroads are meeting already-existing Department of Transportation requirements to emergency preparedness training. As TSA looks to regulate in that area, it is very important that you harmonize that or that one agency takes the field so that you have one set of requirements that pertain.

As Mr. Rojas has pointed out, DHS has acted upon the Executive Order calling for a review. One concern we have, though, is, the document that was accomplished in the *Federal Register* seemed to indicate the focus of that review would be only on rules that were 5 years old or more. With DHS, it has not been in existence that long. Particularly in the area of surface transportation, essentially any regulation that is put out has come out within the past 5 years. So, in a sense, they have taken that off the table.

We would hope that the Department would take a broader look at that action on the President's Executive Order, look at regulations as they exist, and also look at ones that have been legislatively mandated for their necessity at this point.

Mr. ROGERS. Okay.

This will be for Mr. Farmer and Chief Dunham. Currently, TSA has separate offices for freight, rail, and mass transit. Do you support this structure or not?

Chief Dunham.

Chief DUNHAM. I do. I do support it, because we do totally different things, and our challenges are totally different. So I do support having two different structures for——

Mr. ROGERS. How about you, Mr. Farmer?

Mr. FARMER. Sir, I think a split between freight rail and mass transit is sound. We can run into difficulties in coordination, however, with passenger railroads.

Often, freight and passenger railroads operate on the same infrastructure. So it is important there is a common awareness within Government of what the railroads are doing collectively for secu-

rity. Often, because they are on the same routes, freight railroads are doing things that benefit passenger rail security and vice versa. Some of the investments, particularly through the grant programs that this committee has been so instrumental in making happen, have benefits that accrue to freight railroads when passenger railroads are recipients.

In the AAR, we have actually formed a joint committee, a freight and passenger coordinating committee, specifically to ensure that, from a security perspective, as well as operations and safety, freight and passenger rails are working well in concert together.

We would just ask that when TSA considers matters pertaining to rail that they look at it from that integrated approach, that these are not separate channels, that there is many common synergies that can be gained in passenger and freight rail security.

Mr. ROGERS. Okay.

My last question is for Chief Dunham.

Your system is literally a leading system on the security front. It is just very impressive. You know, I feel strongly about your closed-circuit cameras and how far you have come with those and plan to go and, of course, canines, which is my pet issue.

But I would like for you to speak briefly on how the VIPR teams fit into your operations.

Chief DUNHAM. We are very fortunate in Atlanta to have a really good working relationship with our VIPR team with the FAM, under the Federal Air Marshals program. The VIPR teams are a great resource for us, because when you don't have extra resources, you can call the VIPR teams in. They are acclimated to the rail environment, and so they come in, especially for special events, large-scale events, they come in, and they blend in to our environment.

So there are an extra resource, an added resource for us. So we have been really fortunate and have a great working relationship with the VIPR teams.

Mr. ROGERS. Excellent.

That is all I have. The Ranking Member is recognized for 5 minutes if she has any additional questions.

Ms. JACKSON LEE. I thank the Chairman very much.

Mr. Farmer, you have raised some very important issues on how we can make our inspectors really focus in on the work that would secure the railroads. So I raise with you a question of your support for the establishment of a surface inspector office at TSA which would improve oversight and training and would give greater attention to surface programs. The provision is in H.R. 1900.

Mr. FARMER. Interestingly enough, I actually worked at TSA when the program started. At its outset, it was very much coordinated from the headquarters level, which did enable some substantial progress in some key areas to take place: In particular, the arrangements between the railroads and transit agencies on security action items that each agree to, and then the transit and rail communities agreed to have inspectors come in and evaluate those.

In both areas, in freight rail and in mass transit and passenger rail, a substantial value accrued from that coordinated effort driven by well-defined priorities: Assessing action items and producing reports that proved valuable to TSA in developing its programs and certainly proved valuable to railroads, passenger and freight, in

looking at how well they were doing and seeing where opportunities for improvement may exist.

The regional security inspectors that I referenced earlier were actually specifically appointed to achieve the purpose that you have referenced, to bring that oversight, to bring that consistency. In fact, the letters that appoint them are very expressive in how the railroads should be willing and able and, certainly, frequently take advantage of this position. But, unfortunately, it seems that in the actual implementation of those inspectors, the original inspectors have not been able to do the job in the way that the letters indicated they would. They are not even, actually, in the organizational structure for the inspectors in the field.

So some approach that brings back a marrying of the priorities that the field inspectors have with the policies and priorities that are being set by TSA headquarters. Often, that is a concerted effort between the modal divisions, like the freight rail division, mass transit division, with the representatives of the industry—railroad officials, transit officials, people in my position.

So, whatever approach can get us back to that marrying of priorities between the headquarters and the activities in the field is one that I think would be beneficial across the board.

Ms. JACKSON LEE. The intent of the surface inspector office would be just that, and also to focus on the security side of an inspection, things that would prevent harm from coming to the railroad processes and their business. Certainly, I think it is important to look at paperwork, but I think our resources on the Transportation Security Administration should be focused on what is there that is threatening that facility.

Would you agree to that?

Mr. FARMER. Absolutely, ma'am. I think the focus should be on the substance of what is taking place in security in the railroad. It is a very positive story of extensive effort on the freight side and the passenger side to put in place procedures to make that happen.

Documents are important, but when an inspector knows, as in many of those cases I referenced, when an inspector actually knows that the appropriate chain of custody and secure handoff occurred with that tank car and yet makes an issue, a significant issue, of an error in documentation, that is a distraction. That is taking us away from those fundamental priorities that should be driving our program.

Ms. JACKSON LEE. We want to make sure we comply with regulations, but I understand what you are saying. We need to find a way to ramp up one aspect and make sure we are complying with the second aspect, which is paperwork and who transferred it, but find a way to handle that in a manner that doesn't interfere in the real serious work of securing that area. Thank you for that.

Mr. Reese, let me pursue the questions on pipelines. We know that pipeline systems are highly automated, and, therefore, we are hoping that there is technology of the most sophisticated kind that is now being used. So I would appreciate you speaking to the latest security technologies that may be used on pipelines and what discussions, if you have had any, with the Department of Homeland Security regarding dealing with improved pipeline security.

I raise the issue of the incident in Montana, which was not a purposeful act, it was not an act by a terrorist, but our pipeline system is vulnerable. What can we do, what are you doing, what is happening with the security technology for pipelines?

Mr. REESE. Yes, ma'am. First, the overarching challenge with pipelines is they are so geographically diverse, there is so much asset to protect. What it necessitates from the beginning is prioritizing those facilities that are most critical to you. TSA does have a pretty prescriptive process by which operators are to determine. But, ultimately, the operator knows, or should know, what is most at risk and so forth. So it begins with prioritizing those things. Their CCTV systems and the like can be applied effectively. Across miles and miles of pipeline, it is very difficult.

There are some things working in our favor. For instance, because of the DOT and EPA requirements about monitoring rights of way, we do have—in our case, at Colonial, we have aircraft that fly continuously. Those folks are well aware of the security implications, and they know to report abnormalities and so forth.

We still consider our greatest risk to be a third party with a big piece of yellow iron, you know, digging a water well or some kind of trenching that is outside of our company. Basically, a third-party line strike is our greatest risk. But it has the added effect of monitoring for surreptitious activity, or if someone was out there to do us harm, it was detected.

Beyond that, it is a lot of emphasis being placed on the operators to understand what to look for and what to report, suspicious activities. We do reach out to our local law enforcement committees and invite them to our facilities. We get together and look at the facilities and talk, so that those folks have it in their mind what we are, what we are worried about, what we are not worried about, and are able to respond. It is a grassroots, knit-together awareness campaign across the system. We even involve the general public and landowners in that effort.

Ms. JACKSON LEE. Well, I know your challenge is vast. I know pipelines are where we wouldn't even imagine that they are.

Mr. REESE. Yes, ma'am.

Ms. JACKSON LEE. I think, in working with the Chairman, I would like to suggest that this is an important issue for this committee, and working with our stakeholders, that we need to focus on ways that we can ensure the highest level security for this infrastructure that is everywhere.

Let me do a final quick question to the chief.

You made an interesting point, and it was really unique, that you do not get funding from the State of Georgia. So you are dependent on resources, I assume, that you might secure through the fee process, but very dependent on Federal resources. I am reminded, even though it was a strange set of facts, of the Olympics and the incident that occurred there. I know that you all were heavily rail—had initiated or boosted your rail because of the Olympics.

So tell me, if DHS funding was zeroed out—we mentioned the transportation security grants, but I know have you access to others; I think you mentioned UASI grants—how devastating that would be on a large metropolitan area like yours.

Chief DUNHAM. Yes, ma'am. Thank you.

We are in a unique situation, as I stated, that the State of Georgia does not fund transit. So every day is a challenge for operating budget. So you can imagine that when you start asking for target hardening, things, extra CCTV cameras, or intrusion detection for our rail fence line, you know, you have to get in line. So, you know, other things take priority.

So we always have to be conscious of the fact that, if we don't have grant funding for certain items, we don't get them. So if we would not receive any more grant funding——

Ms. JACKSON LEE. Federal funding.

Chief DUNHAM [continuing]. Federal funding, then we would be in trouble. I mean, our system would be left vulnerable for attacks. Of course we would do as much as we could, but, of course, we can do so much more with the Federal funding that we need to receive every day.

Ms. JACKSON LEE. Thank you, Mr. Chairman.

Thank you to the witnesses.

Mr. ROGERS. Just to follow up on the Ranking Member's question, what percentage of your security funding does come from these Federal sources?

Chief DUNHAM. Oh, we have—75 percent of our funding for target hardening comes from grant funding.

Of course, we talked about UASI. We get very little from UASI because they know that we get a lot more from the Department of Homeland Security, and so they go to other agencies first.

Mr. ROGERS. Okay.

The Chairman now recognizes the gentleman from Minnesota from any additional questions he may have.

Mr. CRAVAACK. I will try to make it real quick, Mr. Chairman. Thank you.

Just real quick, after 9/11 unfortunately we have now all been incorporated in part of our National security system. All of us have a due diligence to ensure the homeland security.

With that said, I was kind of wondering, in regards to the different modals here, the "See Something, Say Something" campaign, have you seen that to be fruitful for us?

Could you start off, Mr. Farmer?

Mr. FARMER. Yes, sir, that campaign has been effective in a number of modes of transportation, in particular passenger rail. Amtrak has a very proactive program. A number of commuter railroads around the country promote "See Something, Say Something."

It is actually a program that started with the New York Metropolitan Transportation Authority. It has been widely laid out across the country. Last year, DHS adopted it essentially as a Nationwide program and has introduced it in many critical infrastructure sectors.

So we see it as a very effective means by which the public—which is quite familiar with what goes on in a train as they use it each day because of the time they spend on it—a means for them to understand how to report security concerns.

The freight railroads have programs, as well, that entail reaching out to those who live near their operations or have interest in their

operations and can become additional eyes and ears for security, as well.

Mr. CRAVAACK. Thank you, sir.

Mr. Rojas.

Mr. ROJAS. I would subscribe to your statement that National security is embedded in everybody's psyche, and I would say that everybody is much more alert now as we look out.

We had an incident back in February in the Ranking Member's State, in Lovett, Texas, where a student was actually—a Saudi student was actually arrested after trying to procure some material to develop a bomb. The reason why the student was actually arrested was because an employee of the carrier company noticed that the elements—that the cargo was suspect. He did some research on the person and decided to call. They called in his security team within the company, and they called law enforcement. At the same time, the chemical company also called in the FBI.

So I think there is this level of alertness that is out there that—that is part of that information-sharing component that we are talking about. It goes both ways. It is very important to ensure that that critical information sharing and that component of, how can we communicate with law enforcement to ensure that what we see—if we see something suspicious, that we are able to call it in?

So I think I would agree, I think it is embedded into everybody's psyche now.

Thank you.

Mr. CRAVAACK. Good to know. Thank you, sir.

Chief Dunham.

Chief DUNHAM. Yes, sir. "See Something, Say Something" has become a way of life. It is not just a program. You have to embed it into your everyday operation. So, "See Something, Say Something" is valuable.

One thing we did learn from 9/11 is that we can't do it alone. Even the amount of officers, we can't do it alone. So we need our customers to be our eyes and ears and to help us. So this is something that we can ask them to help us.

We have a very aggressive "See Something, Say Something" program. But not only that, we have a "Not On My Shift" program for our employees. So they help us, as well, because the employees are your first line of defense, and so they tell us what is going on.

So we are very pleased with our "See Something, Say Something" campaign. Tougaloo University just came down last month to actually take a look at our program because it is one of the cutting-edge programs for "See Something, Say Something."

Mr. CRAVAACK. Thanks, Chief. You kind of sparked a memory of when I was in Navy, "Not On My Watch."

Chief DUNHAM. Yes, that is right.

Mr. CRAVAACK. Got it. Okay. Thank you very much.

Mr. Reese, how about in the pipeline industry?

Mr. REESE. You know, most definitely applicable.

You know, pipeline plans are typically threat-based. So there is a baseline of security measures, and then there are additional measures that would be evoked based on threat. However that threat information is obtained, whether it is provided by the Government or whether it is a concerned citizen or it is an employee

who is alert and aware, that information is valuable, and it ought to trigger.

In fact, I would suggest it is the cornerstone of any good, effective pipeline security plan. "See Something, Say Something" is an excellent tenet of security in general.

Mr. CRAVAACK. Good to know. Good information. Thank you for that.

Mr. Chairman, due to the time, I will yield back, sir.

Mr. ROGERS. I thank the gentleman.

Ms. JACKSON LEE. Mr. Chairman, could I just——

Mr. ROGERS. Go ahead. The Ranking Member.

Ms. JACKSON LEE. I can't miss this opportunity. I want to thank Chief Dunham for now publicly announcing a new National effort—"Not On My Shift"—the Chairman and I have just made an agreement, "not on our time on this committee"——

Mr. ROGERS. That is right. Not on our shift.

Ms. JACKSON LEE [continuing]. That anything is going to happen to the Nation's transportation systems. We just put a heavy burden on ourselves. So let's see how fast and furious—"Not On My Shift." I am going to take it to Houston, Texas. That is a great one.

Mr. ROGERS. It is.

Ms. JACKSON LEE. Thank you. I yield back, Mr. Chairman.

Mr. ROGERS. I thank the gentlelady.

Thank all the witnesses for your time and preparation. It has been very helpful.

We have another panel; otherwise, I would keep asking questions. But I would remind all the witnesses that Members may have additional questions. The whole purpose of this hearing is to lay on the record some facts that we then can draw upon to justify changes in the authorization bill. So I know I have some additional questions, and other Members may. I would ask that when those are submitted to you, within 10 days you try to get us back a written response to those.

With that, thank you. This panel is dismissed, and we call up the second panel.

The Chairman now recognizes the second panel. We are pleased to have with us several distinguished witnesses before us today on this important topic.

Let me remind the witnesses that their entire statements will be appearing in the record.

Our first witness is Mr. Nicholas Calio.

How did I pronounce that? I am sure I butchered it.

He is president and chief executive officer of the Air Transport Association.

The Chairman now recognizes Mr. Calio for his opening testimony.

STATEMENT OF NICHOLAS E. CALIO, PRESIDENT AND CHIEF EXECUTIVE OFFICER, AIR TRANSPORT ASSOCIATION OF AMERICA, INC.

Mr. CALIO. Thank you.

Chairman Rogers, Ranking Member Jackson Lee, and Members of the committee, thank you for the opportunity to testify here today.

As the committee undertakes reauthorizing TSA, I think it might be helpful to set a little perspective by recalling why TSA was created to begin with: To protect the United States, its citizens, our economy, and our way of life from terrorist attacks.

The reason I mention this is because, as I travel around in airports, I often observe travelers or passengers who, with the passage of time, don't seem to understand why the screening process is necessary. It is. Can it be better? Yes. ATA is working with TSA to try to improve it.

Effective, efficient security is vital to the United States airline industry in fulfilling our central role in propelling commerce and economic vitality and global competitiveness of the United States. Terrorist attacks either on or through airlines underscore a simple fact: Aviation security is a core homeland security function.

Our airlines appreciate the collaborative relationship we have with TSA and their willingness to partner with us, which has greatly improved the regulatory process and, we believe, aviation security.

ATA supports the risk-based approach to security for passengers, cargo, and crew that Administrator Pistole has endorsed. Allowing TSA to focus its finite resources on that which creates the greatest risk is both good policy and good security. In conjunction with TSA's long-standing strategy of multilayered countermeasures and the incorporation of random measures, this approach allows the agency to further concentrate resources on high-risk passengers and cargo. Targeted security includes differentiating individuals and shippers whose backgrounds are known.

The Air Transport Association, along with the Airline Pilots Association and TSA, has developed a known-crew-member program, which will begin a 90-day pilot program next month at seven major airports. ATA has advocated and discussed with TSA having flight attendants included in that program as soon as possible.

Moving crew out of the regular security line also has a secondary benefit: It speeds up the entire process, which is something that we all, I think, recognize that we need to do. Passengers could also benefit from a known-traveler program. ATA strongly endorses TSA's intention of introducing such a program. In our view, the sooner, the better.

Finally, we support a similar program for cargo. We are working with TSA and Customs and Border Protection toward further risk-based screening of international in-bound air cargo. The goal is for TSA and CBP to receive and process information about shippers earlier in the process so they can do it more effectively and without stopping the flow of goods.

Everything we are discussing here today is about the safe and secure transportation of the people and goods that make America what it is today, connecting small and large communities and connecting America to the global economy. Today, U.S. airlines and their passengers continue to bear the burden of funding a system that benefits the entire Nation. Those who seek to harm our country by targeting commercial aircraft are attacking the entire U.S. population and our way of life, not just the airlines.

Yet, in 2010, passengers and airlines paid DHS $3.4 billion in taxes and fees, $2 billion of which went to TSA. This is a 50 per-

cent increase over what was collected in 2002. It is an enormous contribution from a single segment of the private sector. No other industry or mode of transportation, including anyone on the previous panel, is required to fund their own security, only the airline industry and its passengers. This really has got to change.

In conclusion, the Air Transport Association will continue to work with TSA to evolve our practices to ensure that we have the best possible security so that U.S. airlines can continue to move goods and people to the benefit of our Nation's economy and our global competitiveness. We look forward to working with you and with TSA to reinforce these mutual goals.

Thank you very much.

[The statement of Mr. Calio follows:]

PREPARED STATEMENT OF NICHOLAS E. CALIO

JUNE 12, 2011

INTRODUCTION

As the committee undertakes reauthorizing the Transportation Security Administration (TSA), some perspective is in order by recalling why TSA was created . . . to protect the United States, its citizens, and our economy and way of life from terrorist attacks. I say that because I often observe travelers at airports who, with the passage of time, seem to have forgotten why the screening process in necessary.

A secure aviation system benefits all Americans. Effective, efficient security is vital to a robust and financially sound U.S. airline industry, an industry that propels more than 5 percent of our Nation's Gross Domestic Product. The airline industry's central role in commerce and the economy, and the terrorist strategy to attack America by attacking airlines, underscores a simple fact: Aviation security is a core homeland security function.

At the outset, I would like to state that the Air Transport Association of America (ATA) appreciates the collaborative relationship that we have with TSA. We understand that TSA is the regulator and that airlines are the regulated parties, but TSA's willingness to work cooperatively—to the point of partnership—has greatly improved the regulatory process and ultimately, aviation security.

ATA's priorities in this reauthorization bill include enabling a risk-based, intelligence-driven approach to aviation security that:

- enhances security overall;
- streamlines the passenger screening process, and;
- expedites the movement of goods within the United States and across international borders.

We want to continue to work closely with Congress and the TSA to ensure implementation of the best possible policies to promote commerce and travel while ensuring a secure aviation system.

ATA members understand that security measures are a necessary factor in keeping Americans safe from another terrorist attack. The Christmas day plot in 2009 and the October 2010 cargo plot highlight the fact that aviation is still a terrorist target. However, experience has demonstrated that increased security and facilitation of travel and cargo are not mutually exclusive. Smart investments and policies can make aviation security more effective and efficient and, in turn, enhance travel and trade, thereby benefiting the traveling and shipping public and our economy.

That, in turn, will improve the economic outlook of the U.S. airline industry and realize the potential it holds for job creation. This subcommittee can do its part in achieving that outcome by not imposing new or increased security-related taxes and fees. Commercial aviation is a cornerstone of the U.S. economy. It drives approximately $1.2 trillion in annual economic activity in the United States, roughly 5.2 percent of our Gross Domestic Product (GDP). Airlines are responsible for 10.9 million U.S. jobs and $371 billion in personal earnings. Every $1 million of commercial aviation activity generates 24.6 jobs. Every 100 airline jobs help support some 388 jobs outside of the airline industry.

Airlines in 2010 enplaned more than 720 million passengers and operated more than 10 million flights. Exports by air in 2009 topped $334 billion in value.

ENABLING A RISK-BASED APPROACH TO AVIATION SECURITY

A risk-based approach to aviation security is grounded in solid intelligence and information sharing among Government and industry stakeholders. It proceeds from an examination of the sources, nature, and capabilities of potential threats, and the nature and extent of the security systems and measures in place to defeat such threats. This approach embraces disciplined analysis and recognizes the value it brings to directing the intensity and allocation of security resources where they are most appropriate. It inherently recognizes that "one size fits all" security is inefficient and fails to direct finite security resources appropriately.

Risk-based analysis is a widely accepted approach. The 9/11 Commission, for example, advocated thorough, risk-based analysis in evaluating aviation-security issues. In its final report, the Commission stated:

"The U.S. Government should identify and evaluate the transportation assets that need to be protected, set risk-based priorities for defending them, [and] select the most practical and cost-effective ways of doing so . . ." *Final Report of the National Commission on Terrorist Attacks Upon the United States,* at 391 (2004).

Administrator Pistole's strong endorsement of a risk-based based approach to aviation security in his June 2 testimony before this subcommittee is gratifying. We support his efforts to lead the TSA to develop and employ a more targeted, truly risk-based strategy. This approach, in conjunction with the multi-layered strategy already in place and the incorporation of random measures, will allow TSA to focus its resources on higher-risk passengers and cargo and strengthen the overall level of security while easing the burden of checkpoint security on the vast majority of passengers and focusing cargo-screening resources on shipments that may pose a higher-risk level.

Increased sharing of actionable intelligence information among Government and industry goes hand-in-hand with a risk-based security system. Such collaboration produces smarter security and improves the performance of all parties. ATA's partnership with TSA must extend at least to this degree of cooperation and confidence, and we are pleased that our working relationship with TSA continues to grow in this direction.

SPECIFIC RISK-BASED PROGRAMS THAT SUPPORT SMARTER SECURITY

A. Known Traveler Program.—Administrator Pistole has not only embraced a risk-based conceptual approach to aviation security, he has identified a specific goal of risk-based passenger screening which will allow the TSA to focus limited resources on higher-risk passengers. We commend him for pursuing this concept in order to shrink the "unknown" category of passengers.

Under a Known Traveler Program, passengers would volunteer information about themselves, enabling TSA to create an alternative type of screening for these passengers, which ultimately will reduce the screening lines for everyone. This program should not simply allow certain passengers to go to the front of the line as previous programs have. Rather, TSA should use current databases of information such as Advanced Passenger Information Systems, Global Entry and Secure Flight, as well as other factors, to actually create a different, expedited screening regime for these travelers. As noted above, screening everyone equally squanders limited resources and detracts from focusing on travelers who may present real risks.

B. Known Crewmember Program.—Smarter security includes recognizing individuals who are in positions of trust, whose backgrounds are known and who can be subjected to a different level of security. For example, pilots fly the planes and many are Flight Deck Officers qualified to carry handguns in the cockpit.

Several different systems have been tested and ATA is currently working with TSA and the Air Line Pilots Association (ALPA) to conduct a 90-day test program at Miami, Phoenix, Minneapolis, Seattle, and Chicago airports. This program is based on the current Cockpit Access Security System (CASS) which enables a pilot of one airline to fly in the jumpseat of another airline. This is an historical industry practice that is safely and securely maintained with the help of the CASS system. Under the CASS system, TSA personnel use a pilot's photo identification to verify his/her identity and employment status by checking it against a secure database. The Known Crewmember Program would first move this concept to the security-screening checkpoint to allow pilots to go through an expedited screening. ATA supports expanding the program to include flight attendants once the pilot program proves successful. Eventually, the program will move toward biometric verification. ATA is working with TSA and pilots to test this program and we look forward to the TSA evaluation at the test's conclusion.

C. Known Shipper/Shipment Programs.—The passenger airlines have met the 9/11 Commission Recommendations Act requirement to screen 100 percent of air cargo departing U.S. airports. We achieved this with significant support from the TSA Certified Cargo Screening Program (CCS) which allowed validated air cargo supply-chain participants to prescreen cargo before delivery to the airline dock. In addition, TSA has made good progress in meeting the screening requirement for international in-bound cargo, but dealing with foreign governments/entities creates a unique set of challenges.

Administrator Pistole's work on complex cargo-security issues has been crucial and we commend him for it. In the wake of the October 2010 Yemen cargo bomb plot, TSA has been working closely with cargo carriers to focus on the highest risk cargo—unknown shipments or cargo coming from unknown shippers. Screening cargo piece by piece would shut down the global supply chain so TSA is working with industry and with Customs and Border Protection (CBP) to receive advance information on packages delivered from high-risk areas. TSA recognizes, and we agree, that to preserve the efficient flow of goods, cargo-security enhancements should take place further up the supply chain—it cannot all be done at the airline level without significant disruption and economic harm.

Known Shipper/Shipment Programs leverage DHS information programs and carrier and shipper information to expedite the clearance of shipments that meet certain requirements. ATA supports on-going initiatives to test aspects of such a program and provide valuable information about how to construct an international system that meets commerce and trade needs while efficiently protecting against security risks.

Finally, ATA strongly supports increased use of canine teams as one of the most effective and efficient methods of screening cargo. These teams can be easily deployed and are quick at finding dangerous materials. They may be "low tech," but they are highly effective and efficient. TSA should accelerate implementation of a certification program that enables private canine-screening companies to conduct air screening that meets TSA standards. International canine standards and private-sector options could be leveraged to achieve a higher level of air cargo security on U.S.-bound flights.

DEPLOYING EFFECTIVE TECHNOLOGY AND PERSONNEL

Given the number of passengers and the volume of cargo that airlines transport, technology is an indispensable element in effective and efficient screening. Such technology must perform its screening function in a way that does not disrupt that carriage by air. Our concern is not parochial: Our economy is dependent upon the speed and efficiency of air transportation.

In late 2010, DHS announced more extensive deployment of Advanced Imaging Technology screening equipment. According to DHS, there are 486 AIT machines deployed at 78 airports. The President's fiscal year 2012 budget request indicates that the administration plans to continue their deployment and asks for funding for 1,500 scanners and 535 associated personnel. We encourage the deployment of effective and necessary technology and particularly the Automated Target Recognition software for the body-imaging machines that will only display a person's body outline while identifying an area that needs to be resolved.

ATA also recognizes that workforce considerations are an important element in the security equation and appreciates the unflagging dedication of TSA employees. They are key to civil aviation security in our country. TSA employees have recently voted to bargain collectively. We believe that TSA needs maximum flexibility to respond to threats and that Congress must ensure that any bargaining agreement does not interfere with TSA's ability to perform effectively and nimbly.

COSTS TO PASSENGERS AND THE INDUSTRY SHOULD BE LIMITED

Despite that fact that aviation security is a National security function, airlines and passengers continue to bear the brunt of funding a system that benefits the entire Nation. In 2010, passengers and air carriers paid $3.4 billion to DHS in taxes and fees. This is an enormous contribution from one segment of the private sector for what is a National responsibility. It makes air travel far more expensive for the consumer and is a substantial financial drag on U.S. airlines.

In this respect, ATA strongly opposes any increase in the aviation passenger security fee. U.S. airlines and their passengers contributed $2 billion in taxes and fees to TSA in 2010—a 50 percent increase from the amount collected in 2002. The industry's Federal tax burden on a typical $300 domestic round-trip ticket has nearly tripled since 1972—from $22 to $63. Aviation security taxes and fees now constitute almost 25 percent of the industry's Federal tax burden.

To put this into perspective, the U.S. airline industry's total profit last year was $3.7 billion, just one of three profitable years over the last decade in which U.S. airlines lost $55 billion and shed nearly 160,000 jobs. Due primarily to escalating jet-fuel costs, U.S. airlines lost nearly $1 billion in the first quarter of 2011. Further increasing our tax burden will further undermine the industry's financial health, thereby undermining the overall economic recovery.

Aviation security costs should be borne by the Federal Government. Basic fairness dictates that. Those seeking to harm our country utilizing commercial aircraft are attacking the entire U.S. population and our way of life—airlines are the surrogate, not the ultimate goal of those attacks.

THE U.S. GOVERNMENT SHOULD HARMONIZE INTERNATIONAL SECURITY PROTOCOLS

International harmonization is critical and the U.S. airline industry fully supports the DHS effort to achieve harmonization through the International Civil Aviation Organization (ICAO), something that both Secretary Napolitano and Administrator Pistole have vigorously pursued. However, since there are so many governments with different capabilities, ATA believes that the United States, Canada, the European Union and other major trading partners should achieve a much higher degree of coordination so that procedures can be mutually recognized, thereby diminishing redundant requirements for airlines and their customers. Greater harmonization and mutual recognition would minimize the re-screening of passengers, baggage, and cargo from these countries. It would also allow screening resources to be better deployed and improve the movement of passengers and goods.

CONCLUSION

Since its creation nearly a decade ago, TSA has steadfastly defended the United States from threats to its security. TSA also has developed an extraordinary storehouse of experience that can be applied to continue its mission and, in doing so, continue to improve the efficiency of the processing of passengers and freight in ways which will benefit our economy and our ability to compete globally. ATA looks forward to working with the subcommittee and TSA to realize these mutually reinforcing goals.

Mr. ROGERS. Thank you, Mr. Calio. That was very impressive. We appreciate you being here today.

We now go to our second witness, who is Mark Van Tine. He currently serves as president and chief executive officer of Jeppesen and is testifying on behalf of the General Aviation Manufacturers Association.

The Chairman now recognizes Mr. Van Tine.

STATEMENT OF MARK VAN TINE, PRESIDENT AND CHIEF EXECUTIVE OFFICER, JEPPESEN, ON BEHALF OF THE GENERAL AVIATION MANUFACTURERS ASSOCIATION

Mr. VAN TINE. Thank you, Mr. Chairman.

Good afternoon, Chairman Rogers, Ranking Member Jackson Lee, and distinguished Members of the subcommittee. I appreciate this opportunity to sit before you and speak about the efforts to reauthorize the Transportation Security Administration.

Mr. Chairman, as you said, my day job, I am president and CEO of Jeppesen. I do appear today on behalf of GAMA in my role as the security committee chairman for the General Aviation Manufacturers Association. GAMA represents 72 world-leading manufacturers of fixed-wing general aviation aircraft engines, avionics, and components.

Since the events of September 11, 2001, the general aviation community has worked diligently to increase security measures and awareness of potential threats to the aviation system. Numerous domestic and international initiatives have been put in place

by both Government and industry that substantially mitigate security risks.

There are, however, areas which we believe the committee should focus on for improving security and obtaining operational efficiencies. I have three of note for you.

First is the Large Aircraft Security Program, LASP. The Large Aircraft Security Program has received significant attention from the general aviation community and members of Congress since the notice of proposed rulemaking was published in October 2008. Since introduction of LASP, the industry has raised concerns and actively engaged with TSA to develop a program that appropriately balances legitimate security risks with the rights of citizens to fly their own airplanes. We have made good progress together. GAMA asks that the administration move quickly to incorporate the industry's input and finalize this rulemaking, as it will enhance security without creating negative consequences.

The second is around repair stations. Much like the LASP rulemaking, the GA industry awaits completion of an aircraft repair station security rulemaking by DHS. TSA has put forth rulemaking that would implement security requirements for repair stations in November 2009. We believe it is imperative for TSA and DHS to move forward and complete this rulemaking, which puts in place the kind and the type of risk-based repair for repair station security that is good for the industry and good for the country.

Third is around temporary flight restrictions and access to airspace. Temporary flight restrictions, TFRs, are used specifically to designate airspace around selected sporting events and protect the travel of selected individuals. We understand the desire for implementation of TFRs but suggest that TSA needs to review their impact on the operator community and the opportunities to enhance access for operators that have this security programming in place.

In conclusion, Mr. Chairman and Members of the subcommittee, thank you again for your leadership on these issues and for inviting all of us to testify. I believe it is essential for TSA, industry, and Congress to continue to work together on general aviation security issues to ensure we have an effective security system that supports the business and private use of general aviation aircraft.

Thank you, and I look forward to answering your questions.

[The statement of Mr. Van Tine follows:]

PREPARED STATEMENT OF MARK VAN TINE

JULY 12, 2011

Chairman Rogers, Ranking Member Jackson Lee, distinguished Members of the subcommittee, my name is Mark Van Tine and I am the president and CEO of Jeppesen and the Security Committee Chairman of the General Aviation Manufacturers Association (GAMA). Jeppesen is a wholly owned subsidiary of the Boeing Company and is based in Englewood, Colorado. For more than 75 years, Jeppesen has provided navigation charts, electronic databases, and other information solutions to general aviation and commercial airlines around the world. I appear here today on behalf of GAMA, who represents 72 of the world's leading manufacturers of fixed-wing general aviation aircraft, engines, avionics, and components. Our member companies also operate aircraft fleets, airport fixed-based operations, pilot training, and maintenance facilities world-wide. On behalf of GAMA, I appreciate your convening this important hearing and providing me the opportunity to discuss efforts to reauthorize the Transportation Security Administration.

General aviation (GA) is an essential part of our transportation system that is especially critical for individuals and businesses that need to travel and move goods quickly and efficiently in today's just-in-time market. GA is also an important contributor to the U.S. economy, supporting over 1.2 million jobs.[1] In 2010, U.S. general aviation airplane manufacturers delivered 1,334 airplanes.[2] The total value of these aircraft was $7.9 billion, with 62 percent of that value tied to exports.[3] We are one of the few remaining manufacturing industries that still provide a significant trade surplus for the United States.

Despite the recent economic downturn, general aviation has also been among the most successful industries at creating highly-paid, well-skilled jobs that our economy needs. It is important that Congress and the administration adopt policies that help GA to remain competitive and continue to be a leading contributor to our export base.

GENERAL AVIATION SECURITY

GAMA has long advocated for general aviation security to be based on risk analysis which focuses on measuring threat, assessing vulnerability, and determining potential consequences. When higher risks are identified, appropriate countermeasures and security postures should be deployed in order to mitigate the situation. At the same time, such measures should be operationally feasible and built upon stakeholder input. We also believe that rulemaking should be performance-based and adaptable based on experience and outcomes. Finally, as we have seen in previous efforts by agencies to regulate general aviation, one size does not fit all, meaning it is imperative for Government and industry to work together to secure the GA fleet, and all aircraft in our Nation's skies.

Since the events of September 11, 2001, the general aviation community has worked diligently to increase security and awareness of potential threats to the aviation system. These efforts have been the subject of review by the General Accounting Office (GAO) and Inspector General with the IG concluding that, "The current status of GA operations does not present a serious homeland security vulnerability requiring TSA to increase regulatory oversight of the industry."[4] We appreciate this acknowledgement by the IG and believe we have been a positive, proactive partner in addressing legitimate security threats. It is important to note the GAO commenced another study of GA security in early 2011.

Numerous domestic and international initiatives have been put into place by both Government and industry that substantially mitigate security risk. For instance, some existing domestic programs include:

- The continuous vetting of individual pilots and annual security training for flight instructors.
- An enhanced pilot license that includes the requirement to carry a Government-issued photo identification and a proposal to add a photo to the pilot certificate.
- The DCA Access Standard Security Program that requires the carriage of law enforcement officers on board aircraft entering Washington National via a portal city airport.
- The Twelve-Five Standard Security program for commercial operators of large general aviation airplanes.
- The See Something, Say Something program, and its predecessor Airport Watch, that encourages the GA community to report suspicious behavior.
- Guidelines to assist in identification of suspicious money transactions when purchasing aircraft in accordance with the USA Patriot Act.
- Guidelines published by the TSA to enhance general aviation airport security.
- The TSA Transportation System Sector Risk Assessment process that helps prioritize resources based on threat, vulnerability, and consequence.
- The Least Risk Bomb Location program that designates the area in aircraft where explosives should be placed to limit damage.

Additional international programs include:

- The Advance Passenger Information System that requires general aviation aircraft to file flight information identical to that of commercial operators when entering the United States.
- The International Waiver program that requires foreign registered general aviation aircraft to file a waiver to operate within the U.S. airspace.

---

[1] General Aviation's Contribution to the U.S. Economy, MergeGlobal, 2006.
[2] 2010 General Aviation Statistical Databook and Industry Outlook, GAMA 2011.
[3] Ibid.
[4] OIG–09–69 TSA Role in GA Security.

- All general aviation aircraft arriving from outside the United States are subject to nuclear and radiological material screening by the U.S. Customs and Border Protection Agency.
- The Secure Fixed Based Operator program is a pilot program that provides for pre-departure clearances at foreign locations, like Shannon, Ireland. Aircraft that depart from Shannon meet all requirements, except Department of Agriculture, for entry into the United States.

As a result of the aforementioned programs that focus on domestic and international flights, flight training and pilots, GA aircraft have operated in a safe and secure environment. In general, these programs provide a baseline for GA security in combination with a GA community focused on security. There are, however, areas where we believe the committee should focus on for improving security and attaining operational efficiencies.

LARGE AIRCRAFT SECURITY PROGRAM (LASP)

The Large Aircraft Security Program (LASP) has received significant attention from the general aviation community and Members of Congress since being published in October 2008 as a Notice of Proposed Rulemaking (NPRM).

The LASP proposal is the first time that TSA has attempted to regulate private air travel. We believe strongly that the TSA should take pains to recognize this and ensure that LASP does not infringe on the ability of general aviation pilots and passengers to exercise their freedom to fly by properly introducing targeted requirements.

In this regard, GAMA believes that any final rule should recognize that the vast majority of passengers who board general aviation aircraft are known to the operator and crew, and are made up of employees, guests, family members and clients who typically have close ties to the operator of the aircraft. Unlike commercial operations, passengers in this context are not "revenue service passengers" and unknown, but warrant a uniquely different consideration from a security vulnerability context. In assessing risk, the general aviation "passenger," an individual known to the pilot, represents an inherent and significant risk reduction which should be recognized and accounted for by the TSA as it finishes drafting a final rule for LASP.

Since the 2008 NPRM was published, our industry has raised concerns with the LASP and actively engaged with the TSA to help develop a program that appropriately balances legitimate security risks with the right of citizens to fly their own airplanes.

We have made good progress. During two industry working group session in April and May of 2009 set up by the TSA Transportation Security Network Management (TSNM) office we were able to agree on a framework for the LASP rule. Assistant Administrator John Sammon has committed to build upon what the TSA has learned from these two sessions and issue a second NPRM that incorporates suggestions from stakeholders. On May 12, 2011, TSA Administrator Pistole announced to the GAMA board that the supplemental NPRM had been cleared by TSA.

The framework we have identified in our work with the TSA includes:

- The establishment of a "trusted pilot" system that would require pilots to meet certain requirements before operating their aircraft if that aircraft falls within the TSA-defined scope of LASP.
- The trusted pilot would be responsible for conducting key security functions for flights (like they are for all safety functions) including identity verification of known passengers and an established process for subjecting unknown individuals to vetting through eSecure flight.
- The "securing" of aircraft after landing and before takeoff at all airports.
- The establishment of a sensible restricted items list that takes the place of the prohibited items list originally proposed by the TSA.

We also appreciate the strong support we have received from Members of Congress who have recognized our concerns and urged TSA to develop a more practical and effective approach. GAMA is asking the administration to move quickly to incorporate the industry's input and finalize the rulemaking which is currently pending before the Department of Homeland Security (DHS). Moving forward on this rule with this input will enhance security without the negative impact of the initial NPRM.

REPAIR STATIONS

Much like LASP rulemaking, the GA industry awaits completion of an aircraft repair station security rulemaking by DHS. TSA put forth a rulemaking that would implement security requirements for repair stations in November 2009. GAMA filed comments about how to establish a risk-based program for repair station in a con-

structive manner and we sought to underscore the effect inaction has upon exports of U.S. products and expansion into new markets given the majority of airplane and equipment sales are to foreign customers.

It is worth noting in his recent appearance before this committee, TSA Administrator Pistole stated during questioning that their investigation had found foreign repair station security to be "commensurate with U.S. standards".[5] We concur, and believe it is imperative for the TSA and DHS to move forward and complete this rulemaking which will put in place the type of risk-based for repair station security that we support.

ALIEN FLIGHT TRAINING

The Alien Flight Student Program, established in the Aviation and Transportation Security Act and amended by Vision 100—Century of Aviation Reauthorization Act, creates responsibility for DHS and TSA to perform background checks of foreign nationals seeking flight training in the United States. An interim final rule[6] creating the program was put forth on September 20, 2004, establishing four categories of pilot training candidates based on the type of training being sought.

GAMA believes this rule is not proportional to the risk posed, or mitigated, by the program. For example, the outcome has resulted in international operators electing not to train in the United States, but instead move their training contracts to foreign locations. This hurts U.S. jobs, and the aviation industry as a whole.

GAMA has advocated for policies that properly frame pilot training risk against the requirements placed on the pilot through the interim final rule. We have worked to make better use of agency resources and properly classify "recurrent training" to ensure minimal impact on the ability to renew qualifications for existing pilots who already know how to fly specific aircraft. We believe, however, that it is time to build on the lessons learned during the program's 7 years in existence and develop more targeted requirements, reduce the burden created by TSA having to check the same person multiple times within a couple of months, and allow U.S.-based flight training organizations to compete on a more level playing field.

TEMPORARY FLIGHT RESTRICTIONS AND AIRSPACE ACCESS

Flight restrictions are used to protect critical infrastructure, such as dams and nuclear power plants, and provide a geographic boundary for general aviation aircraft operations. Similarly, Temporary Flight Restrictions (TFR) are used to specifically designate airspace around select sporting events, and protect the travel of select individuals. We understand the desire for implementation of TFR's, but suggest a needed review of their impact on the operator community.

TSA has successfully worked with industry to minimize the ramifications that TFR's created to support Presidential travel. For example, last year the agency worked successfully to mitigate the impact upon flight operations around Martha's Vineyard during a Presidential visit to the area. We applaud this step and believe it can provide an example of how TSA and industry can work together to develop procedures that allow GA operations to continue when TFR's are implemented.

It is also important to note that a number of initiatives permit operators to attain additional security clearances and therefore operate in sensitive areas and these can serve as precedent for easing TFR restrictions as well. In the National Capital Region, general aviation pilots are required to undergo FAA-administered security awareness training each year. Pilots operating in flight-restricted areas, including the Maryland airports Hyde Field, College Park, and Potomac Airfield, are required to obtain additional clearances to access these airports. Similarly, the DCA Access Standard Security Program subjects general aviation operators to a number of requirements, including the carriage of a law enforcement officer on board, and requires departure from one of a few dozen "portal city" airports. The Twelve Five Standard Security Program requires that on-demand commercial aircraft operators using aircraft with a take-off weight above 12,500 pounds to carry out an extensive security program. Finally, the Private Charter Standard Security Program subjects any aircraft with a maximum takeoff weight above 100,000 pounds additional scrutiny of passenger baggage and requires a hardened cockpit door.

We mention these programs because each subjects operators to an additional layer of security. It is our belief that TSA should permit operators with any of the aforementioned clearances, as well as those include under the pending LASP, the ability

[5] Subcommittee Hearing: Authorizing the Transportation Security Administration for Fiscal Years 2012 and 2013, Administrator Pistole Remarks.

[6] 49 CFR Part 1552, Flight Training for Aliens and Other Designated Individuals; Security Awareness Training for Flight School Employees; Interim Rule.

to obtain clearance to operate in TFR's, as they have met a higher level of security requirements. GAMA encourages TSA, and other Government agencies, to evolve how restricted airspace can be accessed by general aviation operators through procedural and possible regulatory changes.

At the same time, GAMA remains supportive of the effort by TSA to broaden general aviation access at DCA. We appreciate that the agency has dedicated time and efforts to expand the number of "portal city" airports and streamlined the existing procedures, as announced in March of this year, both of which have permitted an increase in GA aircraft operations. We are grateful for the effort, but remain cognizant that impediments with other Government agencies remain. We encourage TSA, and other Government and industry stakeholders, to continue their efforts to improve access and maintain security.

GENERAL AVIATION AIRPORT SECURITY

Recently, the GAO released a report entitled General Aviation—Security Assessment at Selected Airports. The report provided a review of 13 general aviation airports using the TSA Security Guidelines for General Aviation Airports which GAMA helped develop. The focus of the assessment was the availability of physical security measures, such as perimeter security, lighting, locked hangars, and closed circuit television, that could prevent unauthorized access to airports. It recognizes the strides that general aviation airports have made, on a voluntary basis, to enhance security.

In response to the GAO study, the DHS states that the "TSA strongly believes that general aviation airports are complying with recommended security measures to the extent that those measures are practical and effective given the unique conditions at each airport, and to the extent funding is available for desired security outcomes."[7]

Most general aviation airports have stepped up and voluntarily established procedures and other mechanisms through which they are hardened. As there are close to 18,000 general aviation airports around the United States we believe that there is no practical way to fence every perimeter or screen every visitor to the airport. Instead, working with the TSA, the community has established procedures and programs that identify suspicious behavior and prevent certain individuals from flying GA aircraft. This includes the:

- DHS "See Something Say Something" program.
- The vetting of pilots like TSA's Alien Flight Program and FAA's review of the pilot registry.
- Specific programs for certain types of operations such as the TFSSP and LASP mentioned previously.

These programs in combination with some basic voluntary steps taken by airports provide the framework within which the GA community's risk can be effectively managed.

TSA'S USE OF SECURITY DIRECTIVES

The general aviation industry is very concerned about the TSA's liberal use of Security Directives to implement new requirements on operators that are not subject to the rulemaking requirements of the Administrative Procedures Act (APA).

The general aviation community strongly supports a risk-based, threat vulnerability approach to securing our National transportation system. However, we have seen the TSA repeatedly use Security Directives to vastly expand existing security requirements without consideration of the implementation challenges, operational impacts, and economic burdens these mandates impose on the aviation industry. Our most recent experience involves the expansion of security credentialing requirements to tens of thousands of pilots and employees at airports and aviation manufacturer facilities without input from these constituencies or due process protections under the APA.[8]

We recognize and respect TSA's authority to issue Security Directives. However, we do not believe that TSA should use Security Directives to make standing policy unless there is a compelling and immediate National security risk that warrants it. This is an issue of great concern to the general aviation community and we urge Congress to implement mechanisms for review of security directives if they are not temporary in nature.

---

[7] General Aviation—Security Assessment at Selected Airports, GAO–111–298.
[8] Security Directive 1542–04–08 revision F issued in December 2008.

CONCLUSION

In closing, Mr. Chairman and Members of the subcommittee, thank you for your leadership on these issues and for inviting me to testify. I feel strongly that if TSA, industry, and Congress continue to work together on general aviation security issues we will put in place an effective security system that does not inhibit the freedom people enjoy today to privately use general aviation aircraft.

Thank you and I would be glad to answer any questions that you may have.

Mr. ROGERS. Thank you, Mr. Van Tine.

The Chairman now recognizes our third witness, Mr. Steve Alterman, currently serving as president of the Cargo Airline Association.

The Chairman now recognizes Mr. Alterman.

STATEMENT OF STEPHEN A. ALTERMAN, PRESIDENT, CARGO AIRLINE ASSOCIATION

Mr. ALTERMAN. Thank you, Mr. Chairman. Good afternoon, Mr. Chairman, Ranking Member Jackson Lee, and Members of the subcommittee. I am delighted to be here today, and we appreciate the opportunity to testify before you as you move to authorize the Transportation Security Administration.

The Cargo Airline Association is the Nation-wide trade organization representing the interests of the Nation's all-cargo carriers. Specializing solely in the transportation of cargo, our members are the primary drivers of a worldwide economy that demands the efficient time-definite transportation of a wide range of commodities.

Every member of the aviation community recognizes that the highest level of safety and security must be a cornerstone of all of our operations. It is also important to understand that the aviation industry is composed of a diverse group of businesses with substantially different operational models. You have heard some from Mr. Calio on the passengers; we have heard some from GAMA. There are a whole host of different aviation models. I believe Mr. Rojas said it earlier with respect to the trucking industry, it is equally true with the aviation industry: One size does not fit all.

Indeed, even within the all-cargo community, there are substantially different operations. Some of our members offer time-definite service and are generally known for their express operations. Other companies concentrate on traditional freight operations, providing the transportation function for the air freight forwarder community. All of these different characteristics are currently taken into account by the Transportation Security Administration, as we all operate under different security directives, different emergency amendments, and different security programs.

Each of these different regulatory requirements is tailored to address the unique threats and vulnerabilities of the separate industry segments. This method of regulating the industry should continue.

This multilayered, risk-based approach to aviation security is clearly appropriate. As TSA Administrator John Pistole said to you on June 2, 2011, "The TSA employs a risk-based, intelligent-driven operation to prevent terrorist attacks." We absolutely agree with this statement.

We believe, however, that this approach to aviation security should go a bit further. We actually think it should be codified in any TSA authorization bill to ensure that the theory and the prac-

tice of regulating the aviation industry based on intelligence-driven, risk-based factors should, in fact, be a cornerstone of the agency itself and should be part of the authorization process.

We also agree with and appreciate Administrator Pistole's commitment to work collaboratively with the stakeholder community to develop the programs necessary to enhance security. To his credit, the administrator has made good on his promise to engage the industry in formulating policy as we move forward.

However, we also believe that the TSA industry communications interface should be strengthened and institutionalized by legislatively establishing the Aviation Security Advisory Committee. This is an advisory committee that was in effect until a couple of years ago. Its charter has run out. It has now being reformed and may have already been technically reconstituted. But we can't gamble that this will happen again, and we urge the committee to move forward in the TSA authorization bill to institutionalize the existence of the Aviation Security Advisory Committee.

I would like to talk just briefly about a couple of things so I don't repeat what Mr. Calio said.

After the incident in Yemen in 2010, a lot of activity took place. The result of that activity was TSA and the industry working collaboratively to put a whole host of new programs in place to secure our international transportation. I would just like to talk about a couple of things that are on-going.

The Department of Homeland Security established air cargo security working groups to deal with what we are going to do as we go forward. We think one of the most promising areas of inquiry is, again, the intelligence-sharing aspect of it. As those working groups move forward, we urge you to let them move forward and encourage them to move forward.

Another one of those committees dealt with how to get better technology and better machines in there so we can screen cargo better. We urge you to continue the funding, but we absolutely recognize the funding problems we have in this country now. So I would like to concentrate a little bit on low-tech rather than high-tech.

A lot was said in the first panel about dogs, and we absolutely agree that the canine program should be encouraged and expanded. We specifically urge that this committee consider forcing the TSA to expand the use of private canines in the screening process and that we don't just rely on TSA dogs, because there aren't enough of them. There is a program we can put in place where TSA could actually certify the dogs and have private screeners do it. We are in strong support of that.

Mr. Chairman, I see my time is up. I would be happy to answer any questions as we move forward. Thank you very much.

[The statement of Mr. Alterman follows:]

PREPARED STATEMENT OF STEPHEN A. ALTERMAN

JULY 12, 2011

INTRODUCTION

Good afternoon Chairman Rogers, Ranking Member Jackson Lee, and Members of the subcommittee. My name is Steve Alterman and I am President of the Cargo Airline Association. We appreciate the opportunity to testify before you today as

Congress moves to authorize the activities of the Transportation Security Administration for fiscal years 2012 and 2013.

The Cargo Airline Association is the Nation-wide trade organization representing the interests of the Nation's all-cargo air carriers.[1] Specializing solely in the transportation of cargo, our members are the primary drivers of a worldwide economy that demands the efficient time-definite transportation of a wide range of commodities. Our industry segment has grown over the years to a point where, in fiscal 2011, it accounted for 87.4% of the Revenue Ton Miles (RTMs) in domestic markets (up from 70.0% in 2000) and 69.1% of the RTMs in international markets (up from 49.3% in 2000). This expansion is expected to continue, with the Federal Aviation Administration estimating a growth rate of approximately 4.5% over the next 20 years.[2]

GENERAL SECURITY CONSIDERATIONS

Every member of the aviation community recognizes that the highest level of safety and security must be a cornerstone of all operations. Failure to recognize this fundamental principle is both bad policy and bad business. It is also important to understand, however, that the aviation industry is composed of a diverse group of businesses with substantially different operational models. For example, Cargo Airline Association members, in their all-cargo operations, do not carry "passengers" in any generally accepted definition of that term, have substantial operations that never touch U.S. soil (sometimes in the livery of foreign carriers), provide substantial support services for the U.S. military and in many cases, have control over the pickup and delivery, as well as the transportation of cargo. Indeed, even within the all-cargo community, there are substantially different operations. Some of our members offer a time-definite service and are generally known for their express operations, while other companies concentrate on traditional freight operations providing the transportation function for the air freight forwarder community. These differing characteristics must continue to be taken into account in developing and implementing security policy. Accordingly, all-cargo air carriers today operate under a different Security Program and different Security Directives than our passenger counterparts or the members of the indirect air carrier community. Each of these different regulatory requirements is tailored to address the unique threats and vulnerabilities of the separate industry segments.

This multi-layered, risk-based, approach to aviation security is clearly appropriate. On June 2, 2011, TSA Administrator John S. Pistole testified before this subcommittee and stated that:

"TSA employs risk-based, intelligence-driven operations to prevent terrorist attacks and to reduce the vulnerability of the Nation's transportation system to terrorism. Our goal at all times is to maximize transportation security to stay ahead of the evolving terrorist threat while protecting passengers' privacy and facilitating the flow of legitimate commerce."

We absolutely agree with this statement. We also believe, however, that this approach to aviation security should be codified in any TSA Authorization legislation and not left to the whim of future Administrators. This codification should clearly indicate that, in issuing regulations and other documents such as Security Programs, Security Directives and Emergency Amendments, the administrator must employ a risk-based, intelligence-driven, approach, taking into account the nature and location of any threats to transportation security, as well as the unique operational characteristics of the various segments of the transportation industry and apply the appropriate security measures to meet that specific threat.

We also agree with and appreciate Administrator Pistole's commitment to work collaboratively with the stakeholder community to develop the programs necessary to enhance security across the transportation system. To his credit, the administrator has made good on his promise to engage the industry in formulating policy as we move forward. Having said that, however, we believe that the TSA/industry communications interface should be strengthened and institutionalized by legislatively establishing the Aviation Security Advisory Committee. While this committee has existed in the past, and we understand that it is about to be reconstituted, there has been a significant gap over the past several years, leaving no formal way for the industry and the agency to communicate. Therefore, we support the provisions

[1] Association members include ABX Air, Atlas Air, Capital Cargo, DHL Express, FedEx Express, Kalitta Air, and UPS Airlines.

[2] Statistics from the *FAA Aerospace Forecast, Fiscal Years 2011–2031,* March 2011.

of H.R. 1447, introduced on April 8, 2011, and urge that this proposed legislation be folded into any TSA Reauthorization bill.

THE LESSONS OF OCTOBER 2010

In late October, 2010, terrorists in Yemen targeted the international supply chain by placing explosive devices aboard two U.S. all-cargo carriers. This plot was thwarted through the work of the intelligence community, but it still sent a wake-up call to everyone in the industry. Subsequent to the foiled attack, all participants in the supply chain, as well as several U.S. Government departments, came together to start a process that has led to substantial improvements in international air cargo security. After a review of the vulnerabilities exposed by the Yemen incident, TSA, working with industry stakeholders, issued a number of new Security Directives and Emergency Amendments designed to address any deficiencies uncovered. While the details of these new provisions cannot be publicly disclosed, we can say that they involve enhancements across the entire range of participants in international commerce—carriers, forwarders, and shippers.

In addition, the incident spurred on-going analyses of other potential enhancements that can be implemented if proven successful. For example, the Department of Homeland Security (DHS) established an Air Cargo Security Working Group to study, and make recommendations on, various aspects of the security puzzle. Perhaps the most promising and certainly most important areas of inquiry involve how to better share and use information developed by the intelligence community and how to develop and certify new technologies to screen high-risk air cargo shipments. With respect to the latter project, we urge Congress, both in the context of authorizing and appropriations legislation, to ensure the funding necessary to continue research on promising new technologies—especially those that might be able to screen consolidated shipments.

It is also important not to overlook "low tech" initiatives to screen air cargo—in both international and domestic markets. Specifically, the use of canines has proven effective in the screening of air cargo, but the use of dogs has been hampered by the relative scarcity of TSA-trained animals. We firmly believe that the use of canines should be aggressively expanded by permitting the use of private, but TSA-certified, canines as a primary screening method. TSA has begun to move in this direction and we encourage accelerated action in this area, both at domestic and international locations.

In yet another development, TSA, in conjunction with U.S. Customs and Border Protection and the air cargo industry, has also begun a significant Pilot Program to determine the feasibility of submitting data on international air cargo shipments earlier than presently required. Such information holds the promise of enabling the Government to target high-risk shipments before they are loaded on aircraft bound for the United States. While initial results of this Pilot Program have been promising, much more needs to be done before any regulatory or legislative conclusions can be reached. At this point, the Program has involved only the express segment of the air cargo community, and even there, only at somewhat remote locations. More work needs to be done in the high volume areas of the express environment and the Program needs to be expanded to the heavy freight environment, as well as to the passenger and air freight-forwarder segments of the marketplace. Therefore, if this committee addresses this Program in any TSA Authorization legislation, we urge that any provisions simply require the continuation of the Program with a Report to Congress at its conclusion. Now is not the time to prejudge the outcome of the Program by mandating any particular pre-flight data submission requirements.

A final lesson of the incidents of October 2010 is that the United States alone cannot ensure the security of international air cargo shipments. The air cargo business is global—and it demands global cooperation to thwart potential terrorist activity. TSA should therefore be encouraged to continue its on-going efforts to work with foreign governments to ensure that these foreign governments adopt security standards substantially similar to those in place in the United States. Over and above this unilateral initiative, every effort should be made to arrive at harmonized international standards for securing the entirety of the supply chain. Such harmonization is necessary both for security and for facilitating the flow of commerce. In a worldwide economy, businesses simply should not be required to adopt widely differing security practices dependent solely on the country of origin of the freight.

CONCLUSIONS

The all-cargo air carrier industry fully understands the importance to maintain the highest possible level of security, while at the same time providing our world-

wide customer base the level of service it demands. In accomplishing these twin objectives, we will continue to work cooperatively with both TSA and CBP to develop and implement the best possible security regime. We urge Congress to assist in this effort by enacting TSA Authorization legislation that establishes guidelines under which TSA must operate, but that does not "over regulate", giving TSA and the industry the flexibility to assess threats and vulnerabilities and to take appropriate action in each individual circumstance.

Thank you very much. I am happy to answer any questions.

Mr. ROGERS. Thank you, Mr. Alterman. We are working to that end, to do just that.

The Chairman now recognizes our fourth witness. Mr. Christopher Witkowski is currently serving as the director of the air safety, health, and security for the Association of Flight Attendants.

The Chairman now recognizes Mr. Witkowski.

STATEMENT OF CHRISTOPHER WITKOWSKI, DIRECTOR OF AIR SAFETY, HEALTH, AND SECURITY, ASSOCIATION OF FLIGHT ATTENDANTS—CWA, AFL–CIO

Mr. WITKOWSKI. Thank you, Chairman Rogers and Ranking Member Jackson Lee, for holding this hearing and allowing us to weigh in on the safety and security issues that are important to flight attendants and National security. We thank Mr. Cravaack for being here, as well, to listen.

My name is Christopher Witkowski. I am director of the Air Safety, Health, and Security Department of the Association of Flight Attendants—CWA. We represent more than 60,000 flight attendants at 23 U.S. airlines.

Before I begin, I would just like to mention that flight attendants, an integral part of the crew in terms of safety and security, have been subject to the same level of screening and background checks as pilots, yet only pilots are being included in a test of the known-crew-member screening process that allows expedited crewmember screening at security checkpoints. We thank the committee for their support of flight attendants, and we hope this committee will continue to exert pressure on TSA to include flight attendants in the program as it moves forward.

I am here to talk about what has happened, or, in this case, what has not happened, to flight attendant security and self-defense training in the 10 years since the horrific attacks of 9/11. Flight attendants are first responders on commercial airplanes responsible for the protection and preservation of the cabin environment as well as the lives of tens of millions of people every year. They are also the last line of defense in the aircraft cabin.

Recognizing their security role, Congress has on separate occasions passed bipartisan laws mandating flight attendant self-defense training. But corporate pressure and agency prejudice have interfered with Congressional intent. I am here to stay that training and equality for flight attendants remains elusive and leaves passenger airplanes unnecessarily vulnerable to attack.

Prior to the 9/11 attacks, flight attendants were instructed to slow down their actions and comply with hijackers, assuming the hijacker wanted to go to a destination or wanted money or notoriety only. Two months after 9/11, Congress passed the Aviation and Transportation Security Act, ATSA, which mandated a change

to the training curriculum and philosophy. No longer was the hijacker intent on going to Cuba. The new hijacker would use the aircraft as a weapon of mass destruction.

Part of the AFA's request to update the training included basic self-defense maneuvers to allow flight attendants defend themselves against a terrorist attack. We are not asking for flight attendants to be certified martial arts experts. AFA worked with the regulators and industry representatives to create a training program that would allow flight attendants to be provided with the appropriate and effective training required to perform their duties.

With the passage of ATSA, AFA also urged Congress to change the requirements for flight attendant security training to include a provision that mandated a set number of hours for the security training. These mandates would have to be enforced so that all carriers would be required to provide the same level of appropriate and effective security training for all flight attendants.

The Homeland Security Act of 2002 required the Under Secretary of Transportation for Security to issue a rule mandating both classroom and effective hands-on situational training covering 10 elements, among them: Appropriate and effective responses to defend oneself, including the use of force against an attacker.

It was Vision 100, the FAA Reauthorization Act of 2003, that eliminated the Department of Homeland Security requirement for TSA to issue a rule requiring both classroom and effective hands-on situational security training. Yet this was done without the Homeland Security Committee review. Thus, Vision 100 left it to the individual air carriers to develop basic security training originally to be done by TSA, including the element related to appropriate responses to defend oneself. Because Vision 100 took away TSA's obligation to develop a basic security training rule for all carriers, it mandated that TSA develop and provide an advanced voluntary self-defense training program.

When we talk about mandatory basic security training in our comments, we are generally talking about only a 5- to 30-minute self-defense training module developed and provided by the air carriers themselves. Air carriers appear to be checking the boxes in relation to the required elements of training. Without TSA-established standards, there exists a wide variance in the amount of security training being allocated to self-defense.

The so-called advanced training that was developed by TSA is the voluntary Crew Member Self-Defense Training. This program offered by TSA is not advanced but, rather, an introduction to basic self-defense. It is a 1-day course conducted throughout the year at various locations and focuses on hands-on self-defense training.

Unfortunately, it is difficult for our members to attend, as it has become harder for them to take time off from work and their flying duties. Flight attendants have been unwilling to attend training that may require them to pay for hotel and meal expenses. The result has been depressed participation in the voluntary Crew Member Self-Defense Training Program. If flight attendants were paid or even if the costs associated with attending were covered, then participation could be higher.

TSA has the authority to implement comprehensive and cohesive security and self-defense training for all flight attendants but has

failed to do so. There should be a mandatory basic counterterrorism training that effectively prepares flight attendants to deal with potential threat conditions, as Congress has required since the enactment of ATSA in 2001.

Despite the best intentions, the ideas put forward by Congress have been weakened and even ignored over time. Comprehensive counterterrorism training must be enacted by Congress in order to ensure implementation of what it has required since 9/11.

As the uniformed crew member tasked by the TSA to defend the flight deck at all costs, according to TSA's Common Strategy, the flight attendant is a target for terrorist to eliminate in order to successfully carry out an attack, the elements of which are stated in the current law. Basic counterterrorism training for flight attendants, if properly required and implemented by TSA, would prepare the flight attendants for potential threat conditions.

Thank you for your attention. I would be happy to answer any questions.

[The statement of Mr. Witkowski follows:]

PREPARED STATEMENT OF CHRISTOPHER WITKOWSKI

Thank you Chairman Rogers and Ranking Member Jackson Lee for holding this hearing and allowing us to weigh in on the safety and security issues that are important to flight attendants. My name is Christopher Witkowski and I am the Director of the Air Safety, Health and Security Department at the Association of Flight Attendants—Communication Workers of America (AFA–CWA). AFA–CWA represents more than 60,000 members at 23 airlines and has been advocating for the flight attendant profession for over 65 years.

I am here to talk about what has happened, or in this case, what has not happened to flight attendant security and self-defense training in the 10 years since the horrific attacks of 9/11. Flight attendants are the first responders on commercial airplanes responsible for the protection and preservation of the cabin environment as well as the lives of over 630 million people annually. Safe and secure travel depends on the ability of flight attendants to identify and respond to threats to passenger health and the safety and security of the aircraft cabin and flight deck.

Flight attendants are also the last line of defense in the aircraft cabin. Recognizing their security role Congress has, on separate occasions, passed laws mandating flight attendant self defense training. While flight attendants have been waiting for mandatory comprehensive security training, flightdeck doors have been reinforced to resist intrusion. Some pilots have been armed under the Federal Flightdeck Officer (FFDO) program. The number of Federal Air Marshalls (FAMs) traveling on flights has increased—although there are still not enough to protect every flight. Flight attendants, an integral part of the crew in terms of safety and security, have been subjected to the same level of screening and background checks as pilots. Yet only pilots are being included in a beta test of the Known Crewmember screening process that allows expedited crewmember screening at security check points. Flight attendants are not yet included in this process.

Flight attendant security issues have continually taken a "coach" seat when it comes to issues surrounding security training and expedited crew screening. Congress intended for flight attendants to receive training but, corporate pressure and agency prejudice have interfered with Congressional intent. I am here to say that training and equality for flight attendants remains elusive.

In 2001 just 2 months after the 9/11 attacks Congress passed the Aviation and Transportation Security Act (ATSA) Prior to ATSA, flight attendants were instructed to slow down their actions and comply with hijacker requests.

ATSA required the FAA to update and improve flight attendant security training requirements to reflect the current security and hijacking situations that flight attendants may face onboard the aircraft.

It was Congress' intention—and AFA–CWA's expectation—that carriers would implement similar, if not identical, training programs. Unfortunately, a 2002 survey of our Safety committee chairs we learned that some airlines were giving their flight attendants a minimal amount of training—in some cases 2 or 3 hours of up-dated hijacking training.

These discrepancies in the security training in the aviation system left flight attendants unprepared for dealing with future terrorist attacks on-board an aircraft in the post-9/11 environment. AFA–CWA has been consistent in our advocacy that all flight attendants, regardless of the carrier employing them, must receive the same level of security training.

With the passage of ATSA, AFA–CWA began to urge Congress to change the requirements for flight attendant security training to include a provision that mandated a set number of hours for the security training. These mandates would have to be enforced so that all carriers would be required to provide the same level of adequate security training for all flight attendants.

In early 2003, air carriers made an unsuccessful attempt to insert a provision into the Omnibus Appropriations Act that would allow carriers to design their own security training effectively making the requirement by the TSA for self-defense training voluntary. Fortunately, Senator John McCain spoke out against this provision and it was defeated. The airlines had also tried to prevent industry-wide standards for the security training and eliminate self-defense training completely.

The airlines finally succeeded in crippling the training requirements with the final language of Vision 100, the FAA Reauthorization of 2003. This was done by eliminating the requirement for TSA to issue a rule requiring both classroom and effective hands-on situational security training. In its stead, Vision 100 created two approaches to self-defense security training. To understand the two approaches of training it is important to understand the basic elements of the law and guidance that are required for crewmember security training. Air carriers are required to provide security training. Vision 100 required air carriers to provide training that included the following elements:

- Recognizing suspicious activities;
- Determination of the seriousness of any occurrence;
- Crew communication and coordination;
- Psychology of terrorists to cope with hijacker behavior and passenger responses;
- Situational training exercises regarding various threat conditions; and
- Appropriate responses to defend oneself.

The carriers provide this basic security training on an annual basis to flight attendants. As noted above, one of the elements is a requirement for "appropriate responses to defend oneself." Vision 100 originally required that TSA establish minimum standards in relation to the training that would be provided to crewmembers including the element related to an "appropriate response to defend oneself."

The subsequent result of the change in language is that the basic security training provided by air carriers in relation to "self defense" training includes anywhere from 5 minutes to 30 minutes of actual hands-on self defense training. So when we talk about "basic" security training in our comments we are talking about a 5- to 30-minute self-defense training module developed and provided by the air carrier themselves.

TSA has the authority to implement comprehensive and cohesive security and self-defense training for all flight attendants but, has failed to do so. There should be a mandatory basic counterterrorism training that effectively prepares flight attendants to deal with potential threat conditions that Congress has required since the enactment of ATSA in November 2001. What is being provided in the voluntary "Crew Member Self Defense Training" (CMSDT) by TSA is not advanced, but an introduction to basic self-defense. The law intended for this type of security training to be provided in mandatory basic security training for flight attendants. CMSDT was intended to train more advanced techniques to volunteers who had previously been trained to "defend themselves, and to demonstrate what they have learned in situational training exercises regarding various threat conditions."

Flight attendant security and self-defense training was meant to provide the appropriate and effective response to a threat to the aircraft. When asked about the effectiveness of the training our flight attendant representatives said it appeared the air carrier met the requirements of the law. However, when asked if their air carrier's security training prepared them to defend themselves and the flight deck should a terrorist attack occur on their aircraft, they've said "No, not really. Only superficially". So while some would say that flight attendants don't want additional security training, the opposite is true. Our flight attendants actually believe that more training is necessary to help defend themselves in order to protect the passengers and flightdeck.

The second training developed in response to self-defense training only is the voluntary CMSDT sponsored by TSA. This is a 1-day (6- to 8-hour) course conducted throughout the year at various locations, such as community colleges around the country and focuses on hands-on self defense training. Unfortunately it is difficult for our members to attend the training as it has become harder for them to take

off from work. The airline bankruptcies which resulted in dramatic pay cuts requiring flight attendants to work more days for the same amount of pay has made it is burdensome for flight attendants to attend the training. Also, flight attendants have been unwilling to attend classes that may require them to pay for hotel and meal expenses. The result has been low participation in the voluntary CMSDT. If flight attendants were paid or even if the costs associated with attending training were covered, then participation could be higher.

Another issue with the advanced voluntary self-defense training is that it is a one-time training that does not include a yearly recurrent training. To fully learn the concepts of the course, a recurrent training program should be made available for flight attendants to reinforce and practice what was taught. AFA–CWA firmly believes that many of the provisions of this voluntary self defense program should be integral parts of an air carrier's basic, mandatory training program.

One flight attendant, when asked to compare the CMSDT to the basic security training being provided by her carrier stated, "I have taken the TSA self-defense class more than 10 times and feel the repetition has greatly enhanced my ability to defend myself. The few minutes in recurrent training does not help flight attendants understand the self-defense moves".

Once Congress ensures that mandatory counterterrorism training, deemed effective by a qualified subject matter expert, such as the lead defensive tactics coordinator for the FAMs or the unit chief of the operational skills unit at the FBI academy at Quantico, is finally provided to flight attendants, CMSDT can indeed provide advanced training. If CMSDT is to remain voluntary, then any crew member who volunteers to enhance their ability to defend National security aboard a U.S. air carrier and attends the training should be compensated for their related expenses and training time, no less than to the extent that FFDOs are compensated or may be so compensated in the future.

Ten years after the 9/11 attacks and almost 3 years after the Christmas day bombing attempt there is still work to be done in all four of these areas.

A subject matter expert looking at the existing statute would ensure that the mandatory basic security training would train uniformed flight attendants, exposed to potential threats in the cabin, on each of the statutory elements of training to give them a reasonable chance of survival, working as a team with the rest of the trained crew and any identified able-bodied passengers, to defend themselves and the aircraft. As the training is provided now, flight attendants are sometimes told that the airline provides security training because they are told to do so by TSA, but that they will likely experience nothing beyond verbal or minor pushing events. Such an attitude of denial in conducting so-called security training is worse than no training at all.

Despite the best intentions, the ideas put forward by Congress have been weakened and even ignored over time. Comprehensive Counterterrorism Training must be enacted by Congress in order to ensure implementation of what it has required since 9/11, but neither the FAA nor the TSA has required. That "Each air carrier providing scheduled passenger air transportation shall carry out a training program for flight and cabin crew members to prepare the crew members for potential threat conditions." As the uniformed crew member tasked by the TSA to defend the flight deck at all costs (Common Strategy II, 2005), the flight attendant is a target for terrorists to eliminate in order to successfully carry out an attack. Basic counterterrorism training for flight attendants, the elements of which are stated in the current law, if properly required and implemented by TSA, would prepare the flight attendants for potential threat conditions.

Mr. ROGERS. I thank the gentleman.

I thank all the panel for those thoughtful opening statements and the time it took to prepare them as well as to deliver them.

Our clocks aren't working, so we are going to wing it and try to stay at 5 minutes.

We heard in the first panel, the ground panels expressed frustration, as we heard in a couple statements on this panel, they expressed frustration of a lack of communication of the threat or the risks that industry folks need to be aware of that TSA has not been sharing as fully as folks would like and working on that.

Another thing that we have heard about, though, are—some industry stakeholders have expressed frustration at technology devel-

opment and procurement, not bringing the private sector in to help find solutions to the problems that folks are facing.

I would ask, and start with Mr. Calio, is your industry being given timely information from TSA as to the technology it needs and foresees needing and asking for feedback as to, you know, how we can get from where we are to where we need to be?

Mr. CALIO. Mr. Chairman, you always think in a situation like this, with these types of situations, that communication could be improved. I would say, in our view, communication with TSA has improved significantly over the last couple years. They are very collaborative with us. They act as a partner with us, in many cases, and share information.

Do we think we would like to have more input at times? Sure, we do. But we have been given a lot of opportunity to have that input.

Mr. ROGERS. Well, I know you mentioned in your opening statement your desire to see not only the pilots and the attendants be able to go through an expedited line but, as you know, the trusted or known traveler. It is my understanding, within the next couple of weeks or so, you are going to hear an announcement with regard to all those things. But I think we all agree that it is going to be a partnership between TSA and the airports to try to make those things work and work effectively, and it is going to benefit everybody.

How about any of the other panelists? Do you feel like you all are being included by the TSA when you are doing, kind of, thinking sessions about what kind of technology we need, how can we procure it and get it in the field?

Mr. Van Tine.

Mr. VAN TINE. Well, I think, as we look at it, I think one of the concerns that we have is the use by TSA of security directives. Certainly, we recognize the importance of using security directives in contingencies and emergencies, but there is this tendency to use it to influence standing policy, rather than working with industry to look at the operational impacts and the consequences of some of those directives.

So, we would ask that the TSA and Congress look at how we can work closer with the industry and not use that as the mechanism for creating a policy.

Mr. ROGERS. Excellent.

Mr. Alterman.

Mr. ALTERMAN. Yeah, I think that, going back to your original question is whether we are being consulted in terms of the technology we need—well, in our instance anyway—to screen freight, the answer is now "yes." What may have been in the past, I think, you know, there may have been some problems, but that is not what we should be concentrating on.

The DHS cargo working groups that were formed within the past year, one of those working groups, sub-working groups, is specifically on the technology, how we get it, what needs to be done, what the monetary/research things are going to be. The industry is intimately involved in that.

So I think the answer to your question is, we are always sometimes frustrated because we want to know everything and we want

to know it yesterday. But with respect to the technology point, we have gotten to a point where we are involved in that process.

Mr. ROGERS. Excellent.

Mr. Witkowski.

Mr. WITKOWSKI. Thank you, Mr. Chairman.

The AFA, in its written testimony, has talked about several other important aviation security issues that need to be addressed.

One of them is a communication device, discreet communication device, that flight attendants could use to communicate with the flight deck pilots in emergency situations that affect the security of the flight. Because every second you lose in response is going to put you more at risk of a successful terrorist attack.

TSA had been looking at this issue because it was required to be looked at in the Homeland Security Act almost 10 years ago. I understand that they had been looking at different types of devices that could be used for communication with the flight deck by the flight attendants. But we were never invited or included in those discussions directly affecting the flight attendants' security aboard the aircraft.

We did participate in a panel that looked at the Federal Air Marshal Communications System, and we contributed to that quite extensively. But as far as the flight attendant issue which we would understood they were discussing, we were not included, and we felt we should have been.

Thank you.

Mr. ROGERS. Excellent.

Mr. Calio—and this will be my last question—we all heard about the Virgin Airlines stowaway. You know, while we are frustrated by that, I like to remind people that we get millions of people right. The fact is, we have human error because humans are running these filters that we use. I am aggravated like everybody else is when we hear about somebody getting through the system. But we also are doing it right in a lot of ways.

But I want to talk about this particular guy for a minute. What type of technology do airlines use at the gate to verify that the boarding pass presented matches that at the flight gate? Does the technology at the gate vary depending on airline?

Mr. CALIO. Yes, Mr. Chairman, it does.

I can't speak for Virgin, where the error occurred, because they are not a member of ours. I can, I think, explain somewhat what happened. You had a dual error: You had a TSA agent error, and then you had a gate agent error.

Mr. ROGERS. Right.

Mr. CALIO. What happened with the gate agent, when he scanned the boarding pass, it showed an error. Virgin's scanner shows—just a red light goes on. For whatever reason, that gate agent did not check any further as to what the problem was.

For ATA-member airlines, when a gate agent scans the bar code, if it comes up red, there could be as many as a dozen or more error codes that come up, which will then allow the gate agent to figure out what is wrong.

I would point out, in this particular case, this same individual who was traveling on Virgin was stopped at the gate by a Delta agent, which is when he was arrested by the FBI.

Mr. ROGERS. Right. That is my point. On this particular case, this is very frustrating because there were several elements of human failure. But thank you for that feedback.

With that, I will shut up and let the Ranking Member ask her questions.

Ms. JACKSON LEE. Not at all, Mr. Chairman. Thank you very much for what I thought were some very instructive questions.

Let me thank all the witnesses for their very, I think, constructive remarks.

I would like to thank the cargo association, Mr. Alterman, for your support of the Aviation Security Advisory Committee. I believe that that is an important issue. Both Mr. Thompson and myself, the Ranking Member, have requested TSA to establish that. We are hoping to codify that in legislation in working with the Chairman of this committee.

In the earlier questioning, we said, not on our watch—at least, I offered those words—as we look at the transportation system throughout America. I think there are a lot of points that have been made that would help us move forward together. That is what I think is most important, a public/private partnership.

Earlier today, I had the opportunity to speak to an industry group on the issue of cargo security. Our commitment there, along with the Secretary of Transportation, was Government and the private sector working together. I want to thank them for their policy hearing.

But I will always look to the rightness of some of the things that TSA does. On their pilot program—I am not sure if this is a lucky number—it seems like the State of Alabama and the State of Texas has been left out. The Chairman did not ask me to mention that. But I would wonder why that is the case. I would like a review. I don't see why we couldn't have more in the pilot program. Maybe there will be someone here to—not the panelists, of course—but if we can get with TSA on that choice. I think to include additional southern cities would be very helpful, and busy cities as well.

But as I move forward, let me try to focus in on some of the points that have been made in particular about issues that are of concern.

The repair stations, I think, Mr. Van Tine, you spoke about. We have no light here, so let me try to encourage your answer. Is there an inconsistency in our oversight of the repair stations? Would you want to articulate that again, please?

Mr. VAN TINE. So, again, when you look at the industry and we produce, a large percentage of our product is going overseas to international locations and are operated on an international basis. So what we are looking for is consistency in application of those security requirements.

The TSA has reviewed that and believes that there is consistency. I believe that when Administrator Pistole testified here a couple weeks ago that he noted that. So we are looking for that, that that rulemaking be implemented and that that be put in place so that there is that consistency.

Ms. JACKSON LEE. You believe you have sufficient input on the rulemaking, that it is one that is going to be constructive in oversight of those repair stations?

Mr. VAN TINE. Yes, we do, and we support it.

Ms. JACKSON LEE. You are speaking about foreign repair stations?

Mr. VAN TINE. I am.

Ms. JACKSON LEE. All right. Because that has been a constant source of concern for this committee, as you well realize that it is also a source of potential threat. I think we need very, very strong oversight, but we need consistency. Is that your position?

Mr. VAN TINE. That is our position, yes.

Ms. JACKSON LEE. Right.

Let me go to the flight attendants—I have just heard the bell here—very quickly.

First, let me say to personally to Mr. Witkowski that I have been consistently fighting for what I think is common sense. There are two aspects to that.

One, I would encourage that flight attendants have the opportunity to have the same security access or ease of access that our pilots do. I have never seen a plane take off without a pilot or the sufficient flight attendants. I have been on planes when we are waiting for flight attendants. So I know that they are not flying but they are part of the team. I don't see why we cannot get a full understanding of that issue.

Ms. JACKSON LEE. So can you explain the devastation or the potential danger of an untrained flight attendant for some of the more serious incidents that might occur?

I imagine that the flight attendants that were on the Northwest Airlines December 25 flight into Detroit were using their basic instincts, unless you are going to tell me that they had gone through the training that I have asked for them to go through. If they did not, say they did not.

Mr. WITKOWSKI. Well——

Ms. JACKSON LEE. They did not go through a higher level of training, is that correct?

Mr. WITKOWSKI. They didn't go through the higher level of training——

Ms. JACKSON LEE. But they used their instincts, and that training might have helped even more. So tell me what happens without that higher level of training?

Mr. WITKOWSKI. Well, their reaction was more of a firefighting reaction, in terms of trying to get the fire out that the terrorists had begun when they were trying to use the explosives.

Ms. JACKSON LEE. Right.

Mr. WITKOWSKI. But if there is a terrorist attack which involves deadly force, the flight attendants will be the first to go, as some were on 9/11.

TSA had tried to make a rule saying that you could allow some items on board the aircraft, like scissors, that would have less than, I think, 4½ inches or 5 inches of a blade. But the idea of that was that, when you punch that in, you are not likely to kill someone. Well, the problem is what they do if they slice the arteries in the neck. Someone can bleed out in a matter of 10 or 15 or 20 seconds.

So if flight attendants don't get that basic training to react instinctively, or as trained—I am sorry—to block, you know, those

areas where they can be killed and they can bleed out, then they will die and the terrorists will have control of the cabin. Because we never know what other passengers or—FAMs are not on most flights. So you are not going to be able to control that, and the terrorists will have control of the cabin.

Ms. JACKSON LEE. So what is your argument, what is your bottom line about the enhanced training?

Mr. WITKOWSKI. What is needed in the enhanced training?

Ms. JACKSON LEE. What is your bottom line on the enhanced training? How important is it?

Mr. WITKOWSKI. It is absolutely critical to National security.

Ms. JACKSON LEE. How difficult do you think it is for airlines to do so?

Mr. WITKOWSKI. It is not difficult. In fact, as I mentioned earlier, the Homeland Security Act language, if that language was just reinstated in the law, TSA was going forward with that in developing a program that the carriers could have enacted in 2003 and beyond.

Ms. JACKSON LEE. How costly, just from your own guess? Do you think it would be enormously costly?

Mr. WITKOWSKI. I don't think it would be enormously costly, in terms of having that kind of a program. One of the recommendations we made in our written testimony was that you would make sure that someone such as the head of defensive tactics for the Federal air marshals would ensure that it was effective training, or someone that deals with——

Ms. JACKSON LEE. While they are in their basic training, it could just be a continuation. Would you assume that that could work?

Mr. WITKOWSKI. Yes. Yes. There could be a recurrent training. Once you get down—you have to train in the initial training so that the flight attendants can react immediately, so they have built muscle memory from the training in order to react if they are attacked in the cabin.

Ms. JACKSON LEE. Well, let me move quickly. Let me just say that I am interested in the issue of the security access. Hopefully we will work with TSA to find out how that can be expanded.

I have two quick questions for Mr. Calio and Mr. Alterman. I apologize, too, if the name pronunciation is not correct.

But after 9/11—and let me just say, I have a great appreciation for airlines. It brings grandmas together with grandchildren. If you go into the airports, you know, people are generally happy because they are going somewhere and they are going to get there quickly.

I did not and I don't believe any Member of Congress hesitated one moment after 9/11 to bail out the airlines. I was here then. I understood the depth of devastation and the cry from airlines that they needed a very large bailout, and this Federal Government did so. So the idea of paying for security is what patriots do. Patriots stand up for their country. There is absolutely no other way that we can provide for security without that assessment.

Now, whether we increase it, I have an open mind. I am interested in not being enormously burdensome. But I cannot in any way accept the fact that it is not the responsibility of the airlines and those of us who are passengers—and we do pay it. It is passed

through to us. The passenger fee is passed through to us, so it doesn't impact airlines at all.

But what I would like to find out is this issue of the recurrent basic training to flight attendants and the idea of this enhanced training. What would be the problem with that, Mr. Calio? If you could pronounce your name correctly so we could——

Mr. CALIO. You got it right the first time. "Calio."

Ms. JACKSON LEE. "Calio." Thank you.

Mr. CALIO. But I have heard it many different ways.

Ms. JACKSON LEE. Well, we shouldn't do that. So, "Calio." Thank you.

Mr. CALIO. Thank you.

I would say first that the safety of our crews and passengers are always our highest priorities, and we won't compromise that.

You know I believe that we have a disagreement about whether the enhanced training is necessary. We provide basic training and defensive techniques as part of our comprehensive flight attendant training. We don't believe that training in more aggressive measures would provide measurable security benefits based on all the multilayered security procedures and processes already in place.

Ms. JACKSON LEE. I respect that. But why not have it to use it if necessary? That is really the question that is not being answered. Why not have it to use it if necessary?

I think the counter—the complement to that, of course, is the appropriate use of it. I believe that you have well-trained, well-selected flight attendants that would have the right judgment. Certainly, we wouldn't want to use it on a passenger that got up to the restroom at the wrong time if all they were doing was going to the restroom. But I do think it is appropriate, in the climate that we are living in, to have that. I would like to keep an open mind. I am going to convene a meeting of the airlines, that I hope maybe the Chairman will join with me, on that issue.

Let me finish by just asking Mr. Alterman—thank you for your answer.

Let me ask Mr. Alterman, we had packages that you know that were coming in from Yemen on flights that were cargo. It opened our eyes. Some of us had our eyes open before, but it opened our eyes to the eye of the storm that cargo planes and your staff and your personnel are in. What should we do more on the cargo security side?

Mr. ALTERMAN. Thank you.

I think that a lot of the answer to that question is what has been done. You are absolutely correct, it opened all of our eyes. Terrorists are not dumb. Terrorists are looking to exploit weaknesses. It is virtually impossible to figure out everything that they might do in the future. So this threat in Yemen was an eye-opener for all of us.

What it did immediately, it set into motion a series of events whereby the Transportation Security Administration, in conjunction with the industry—and I have to give them credit. I am beginning to feel like an apologist for TSA, and I don't want to do that, I will probably get fired. But, to their credit, they worked with the industry after the Yemen incident——

Ms. JACKSON LEE. That is good.

Mr. ALTERMAN [continuing]. To try to figure out where the vulnerabilities are, what went wrong, and how do we avoid them in the future.

The results of that work, I mentioned some of them. Some of them are on-going projects that are on-going through DHS in the working groups, that are on-going in the pilot programs that have been described by Mr. Calio, to try to identify freight in advance of it being loaded on the plane.

But let me go back to what was done immediately, because I think that was very important and very unusual. TSA issued a series of new security directives and emergency amendments as it began to find out more information. What we learned clearly from that incident is that intelligence is the best way of thwarting terrorists. Those packages, all of them, were screened three times. Guess what? They looked like printer cartridges. They were actually thwarted by the intelligence efforts of people overseas.

So one of the things we learned and we have tried to implement—and we have talked about it before—is we need to get better intelligence sharing. We need for the Government to share with itself, among itself, and transmit that to the industry as quickly as possible.

But over and above that, what we learned is that we need, again, to employ the risk-based system, to understand that a package from Yemen may not be the same as a package from Dubuque, Iowa; that we need to take different measures based on the threat, both on the location and the shipper; we need to get a better trusted-shipper program overseas so that we know who we are dealing with; and when we don't know who we are dealing with, we need to take more intrusive and better care of our freight.

Mr. ROGERS. I hate to cut you off, but we have got 3½ minutes to get over to the floor. I want Mr. Cravaack to be able to ask a question before we leave.

Ms. JACKSON LEE. Thank you, Mr. Chairman.

Thank you to the witnesses.

Mr. CRAVAACK. Thank you, Mr. Chairman. It is more of a statement than anything else.

Mr. Calio, I appreciate your being here today. Both as an airline pilot, a commercial airline pilot, and also a Federal flight deck officer, I have gone through a lot of different training in this industry. I really think it is imperative, what you brought out in your written testimony, that the air crew, flight attendants and pilots, know who is on their aircraft. It is imperative. I would just echo that, and I would just compliment you on that.

Mr. Witkowski, I have just a couple quick questions for you because, unfortunately, it is going to be abbreviated. I am a strong proponent of "known crew member." Flight attendants are part of that crew, and I strongly support that.

Mr. WITKOWSKI. Thank you.

Mr. CRAVAACK. But with that said, you are proposing additional training. Some of the words you used are "flight attendants must know how to respond to deadly force; it is imperative to National security."

But as this rule is written right now, sir, what I have a very big contention with, is that additional training, as proposed, which pro-

hibits any testing and allows any crew member to opt out if they do not wish to physically participate—is that correct, sir, or am I reading this wrong?

Mr. WITKOWSKI. No, the Homeland Security Act that I referred to did allow a crew member who believed that they couldn't take the hands-on self-defense training was allowed to opt out. That was in the Homeland Security Act language.

Mr. CRAVAACK. Okay. I have a real big problem with that, especially going through Federal flight deck officer training and some of the training I have gone through. If they are going to be a vital member of the team, as you proposed, in making sure that they know how to use deadly force, and it is imperative to National security—especially the deadly force. You don't want to engage unless you know what you are doing.

The big thing is—and I have gone through enough physical training to understand this—as much as you need to know to give a punch or a block, you have to know how to take one and respond.

So that was just my point. Did you have something to say, sir?

Mr. WITKOWSKI. I was just going to say that the way TSA began to implement that, before it was taken away by the following Vision 100, was that they were going to ensure that all the crew members got the training or some level of self-defense training so they could protect themselves.

Mr. CRAVAACK. Yeah.

Mr. ROGERS. Great.

Mr. CRAVAACK. Okay, I am sorry. I apologize. We have to go vote. I yield back.

Mr. ROGERS. I apologize to all of you. I have so many more questions. Obviously, we all do. We have 54 seconds to get across the street.

Having said that, we are leaving the record open for 10 days. I know I am going to supply some questions to you all, and I know the Members will.

Again, as I told the first panel, all of this is about putting stuff on the record to support our writing of the authorization, so your answers are very important, just as your testimony and presence is. So I really appreciate that.

I want to thank the witnesses for their time, and I apologize for the delay and having to leave early. The Members of the committee, again, will get you questions, and I appreciate your answering them.

With that, this committee stands adjourned.

[Whereupon, at 5:13 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTION FROM CHAIRMAN MIKE ROGERS FOR THOMAS L. FARMER

Question. Mr. Risch in his testimony stated that the training provided to rail employees consists primarily of watching a brief video, and is not substantive enough for the needs of the employees. Can you outline in detail the security training initiatives of your passenger and freight rail members? Including information that responds to the following:

- What does the training consist of?
- How often do employees receive training?
- How is the training assessed and validated?

Answer. Response was not received at the time of publication.

QUESTIONS FROM RANKING MEMBER SHEILA JACKSON LEE FOR THOMAS L. FARMER

Question 1. Recently the Department of Homeland Security issued new surface security grant guidance, which according to DHS will focus on highest-risk assets. I am concerned that the grant dollars may be concentrated only on major metropolitan cities. Can you please shed light on the how commuter rail will be impacted by the new grant guidance? How will security training programs relying on this funding be impacted?

Answer. Response was not received at the time of publication.

Question 2. Do you believe the Department's grant priorities are harmonized with State and local preparedness priorities in response to enhanced security of the transport of hazardous materials?

Answer. Response was not received at the time of publication.

Question 3a. There appear to be more operations between TSA and transit agencies in conducting exercises and testing technology.

Can you please share some of your experience with efforts under way between TSA and rail stakeholders to enhance security? How are VIPER teams facilitating our security goals in the field? How can this relationship and collaboration improve?

Answer. Response was not received at the time of publication.

Question 3b. Have you perceived any changes in TSA's approach to surface transportation security following the discovery that al-Qaeda has allegedly considered U.S. rail targets?

Answer. Response was not received at the time of publication.

Question 4. The last TSA authorization bill, H.R. 2200, established an office of surface transportation at TSA. Do you feel this is a reasonable provision that would give surface security programs more prominence at TSA?

Answer. Response was not received at the time of publication.

Question 5. Earlier this month, TSA announced that it would be reinstating the Aviation Security Advisory Committee (also known as ASAC). One of the primary functions of the advisory committee is to facilitate stakeholder input across TSA security policies as they pertain to aviation security programs. As some of you have testified before us here today, DHS has facilitated industry stakeholder meetings through its Infrastructure Protection initiatives; however, these groups would generally focus on big-picture items and funding issues associated with surface and mass transit programs. Therefore, would you support the notion that a standing committee with active TSA leadership housed within TSA, would benefit industry groups interested in active participation in the development of surface and mass transportation security policies?

Answer. Response was not received at the time of publication.

QUESTIONS FROM RANKING MEMBER SHEILA JACKSON LEE FOR MARTIN ROJAS

Question 1. TSA has been working towards growing situational awareness programs for truckers that train truckers and mass transit professionals to recognize

and report security threats. In you statement you call for improved coordination efforts and less regulations for your members. In an effort to improve security goals, how can TSA incentivize your members to participate in the situational training programs made available today?

Answer. Response was not received at the time of publication.

Question 2. Please provide comment on the recent announcement that the United States and Mexico have an accord on Mexican truck driver operations in the United States, which includes new monitoring procedures for trucks and traffic sign proficiency requirements for truck drivers?

Answer. Response was not received at the time of publication.

Question 3. Are you aware that TSA's Transportation Threat Assessment and Credentialing division is considering an internal reorganization, as well as a transportation worker credentialing "harmonization" that may change the cost to industry and workers for transportation security credentials? Have you been consulted by TSA on this process? Are you concerned that harmonization could lead to increased fees for transportation security credentials?

Answer. Response was not received at the time of publication.

QUESTION FROM CHAIRMAN MIKE ROGERS FOR WANDA Y. DUNHAM

Question. A former CIA senior operations officer recently published a book titled "Willful Neglect: The Dangerous Illusion of Homeland Security"'. This book specifically identifies an increase in bomb-sniffing dogs and random bag checks as a critical piece to improving mass transit security. How can TSA help transit systems to expand the use of canines, and provide guidance as to best practices in canine deployment?

Answer. Response was not received at the time of publication.

QUESTIONS FROM RANKING MEMBER SHEILA JACKSON LEE FOR WANDA Y. DUNHAM

Question 1. In terms of responding to an emergency situation, give us your thoughts on how communications and information sharing has changed over the past few years between you, other law enforcement agencies, and Federal and State authorities.

Answer. Response was not received at the time of publication.

Question 2. Please describe the types of projects and operations at MARTA that are funded by Transit Security Grant Program (TSGP) funds.

Answer. Response was not received at the time of publication.

Question 3. Do you have any comments on the new grant guidance for the TSGP?

Answer. Response was not received at the time of publication.

Question 4. Do you think reductions in TSGP funding could impact security at transit systems Nation-wide?

Answer. Response was not received at the time of publication.

QUESTIONS FROM RANKING MEMBER SHEILA JACKSON LEE FOR RAYMOND REESE

Question 1. Does TSA need more authority to further secure the Nation's pipelines?

Answer. Response was not received at the time of publication.

Question 2. How often do you participate in security exercises with the Department of Homeland Security, Department of Transportation and local first responders? How do you ensure that first responders are actively engaged in security programs with industry?

Answer. Response was not received at the time of publication.

QUESTIONS FROM RANKING MEMBER SHEILA JACKSON LEE FOR JOHN RISCH, III

Question 1. TSA has recently made some structural and resource changes to the Transportation Security Inspector program, including changes in training and lines of report. Have your members been able to engage with TSA on the Transportation Security Inspector program, changes to its organization structure and how this program will play a vital security role across rail operations?

Answer. Response was not received at the time of publication.

Question 2. What changes in TSA surface security programs and policies would better equip rail workers to recognize and address terrorist threats?

Answer. Response was not received at the time of publication.

QUESTIONS FROM RANKING MEMBER SHEILA JACKSON LEE FOR NICHOLAS E. CALIO

Question 1. We have heard from TSA that they have data showing that checked baggage fees are contributing to a dramatic increase in carry-on bags, which presents a security problem for screeners at the checkpoint and flight crews at boarding. The media has reported that air carriers will receive 3.4 billion dollars in checked baggage revenue. What is ATA's position on this issue and what are air carriers willing to do to help address the situation?

Answer. Response was not received at the time of publication.

Question 2. Is it the air carrier's responsibility to regulate carry-on bag size? Do you agree with some stakeholders that increased carry-on bag volume adversely impacts security by increasing congestion at security checkpoints and on the aircraft, and by reducing the ability to detect anomalies in more densely packed carry-on bags?

Answer. Response was not received at the time of publication.

Question 3. Are your member carriers concerned at all with the proposed reorganization of the Transportation Threat Assessment and Credentialing division at TSA and the associated "harmonization" of the credentialing process, the result of which may lead to increased fees for aviation worker credentialing?

Answer. Response was not received at the time of publication.

Question 4. What is your assessment of the progress being made on the statutory requirement that air carriers screen all inbound cargo on passenger planes for explosives?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIRMAN MIKE ROGERS FOR MARK VAN TINE

Question 1. In your testimony you talked about how TSA's security directives tend to function as standing policy.

What processes are currently in place to allow your industry to request a review of existing security directives?

Answer. Response was not received at the time of publication.

Question 2. In your testimony you also mentioned the redundancies in the background checks that TSA performs for alien students attending flight schools.

Can you outline in detail what changes you would like to see TSA make to this program in order to allow U.S. flight schools to be more competitive while maintaining security?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIRMAN MIKE ROGERS FOR STEPHEN A. ALTERMAN

Question 1. In your testimony you highlighted the importance of sustained support to develop new technologies to screen consolidated shipments. How can TSA better collaborate with your industry to support this effort?

Answer. Response was not received at the time of publication.

Question 2. What changes, if any, would you like to see made to the Air Cargo Security Working Group to improve its impact?

Answer. Response was not received at the time of publication.

QUESTIONS FROM RANKING MEMBER SHEILA JACKSON LEE FOR CHRISTOPHER WITKOWSKI

Question 1. Are flight attendants a lower risk population that should participate in any crew access program to expedite security screening—the one that pilots are participating in?

Answer. Response was not received at the time of publication.

Question 2. Please explain why it is difficult for flight attendants to access the advanced self-defense training for crew.

Answer. Response was not received at the time of publication.

Question 3. Some have called the advanced crew training "Judo" training that is not effective. Do you agree?

Answer. Response was not received at the time of publication.

Question 4. Do you feel that like pilots, flight attendants are a low-risk population that should participate in any programs to expedite flight crews around security checkpoints so that TSA personnel can focus screening resources on higher-risk populations?

Answer. Response was not received at the time of publication.

Question 5. In the 10 years since the 9/11 attacks, how has the flight attendant profession changed in terms of security training and preparation? Do flight attend-

ants feel that they have more tools and resources today than before to disrupt an in-flight terrorist attack?

Answer. Response was not received at the time of publication.

○