

**TSA OVERSIGHT PART III: EFFECTIVE SECURITY  
OR SECURITY THEATER?**

---

**JOINT HEARING**  
BEFORE THE  
**COMMITTEE ON OVERSIGHT  
AND GOVERNMENT REFORM**  
AND THE  
**COMMITTEE ON TRANSPORTATION  
AND INFRASTRUCTURE**  
**HOUSE OF REPRESENTATIVES**  
**ONE HUNDRED TWELFTH CONGRESS**

SECOND SESSION

MARCH 26, 2012

Printed for the use of the Committees on Government Reform and  
Transportation and Infrastructure

**Serial No. 112-174**  
**Committee on Oversight and Government Reform**  
**Serial No. 112-78**  
**Committee on Transportation and Infrastructure**



Available via the World Wide Web: <http://www.gpo.gov/congress/house>  
<http://www.house.gov/reform>

U.S. GOVERNMENT PRINTING OFFICE

75-743 PDF

WASHINGTON : 2012

---

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

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

DARRELL E. ISSA, California, *Chairman*

DAN BURTON, Indiana	ELLJAH E. CUMMINGS, Maryland, <i>Ranking Minority Member</i>
JOHN L. MICA, Florida	EDOLPHUS TOWNS, New York
TODD RUSSELL PLATTS, Pennsylvania	CAROLYN B. MALONEY, New York
MICHAEL R. TURNER, Ohio	ELEANOR HOLMES NORTON, District of Columbia
PATRICK T. McHENRY, North Carolina	DENNIS J. KUCINICH, Ohio
JIM JORDAN, Ohio	JOHN F. TIERNEY, Massachusetts
JASON CHAFFETZ, Utah	WM. LACY CLAY, Missouri
CONNIE MACK, Florida	STEPHEN F. LYNCH, Massachusetts
TIM WALBERG, Michigan	JIM COOPER, Tennessee
JAMES LANKFORD, Oklahoma	GERALD E. CONNOLLY, Virginia
JUSTIN AMASH, Michigan	MIKE QUIGLEY, Illinois
ANN MARIE BUERKLE, New York	DANNY K. DAVIS, Illinois
PAUL A. GOSAR, Arizona	BRUCE L. BRALEY, Iowa
RAÚL R. LABRADOR, Idaho	PETER WELCH, Vermont
PATRICK MEEHAN, Pennsylvania	JOHN A. YARMUTH, Kentucky
SCOTT DESJARLAIS, Tennessee	CHRISTOPHER S. MURPHY, Connecticut
JOE WALSH, Illinois	JACKIE SPEIER, California
TREY GOWDY, South Carolina	
DENNIS A. ROSS, Florida	
FRANK C. GUINTA, New Hampshire	
BLAKE FARENTHOLD, Texas	
MIKE KELLY, Pennsylvania	

LAWRENCE J. BRADY, *Staff Director*

JOHN D. CUADERES, *Deputy Staff Director*

ROBERT BORDEN, *General Counsel*

LINDA A. GOOD, *Chief Clerk*

DAVID RAPALLO, *Minority Staff Director*

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

JOHN L. MICA, Florida, *Chairman*

DON YOUNG, Alaska  
THOMAS E. PETRI, Wisconsin  
HOWARD COBLE, North Carolina  
JOHN J. DUNCAN, JR., Tennessee  
FRANK A. LOBIONDO, New Jersey  
GARY G. MILLER, California  
TIMOTHY V. JOHNSON, Illinois  
SAM GRAVES, Missouri  
BILL SHUSTER, Pennsylvania  
SHELLEY MOORE CAPITO, West Virginia  
JEAN SCHMIDT, Ohio  
CANDICE S. MILLER, Michigan  
DUNCAN HUNTER, California  
ANDY HARRIS, Maryland  
ERIC A. "RICK" CRAWFORD, Arkansas  
JAIME HERRERA BEUTLER, Washington  
FRANK C. GUINTA, New Hampshire  
RANDY HULTGREN, Illinois  
LOU BARLETTA, Pennsylvania  
CHIP CRAVAACK, Minnesota  
BLAKE FARENTHOLD, Texas  
LARRY BUCSHON, Indiana  
BILLY LONG, Missouri  
BOB GIBBS, Ohio  
PATRICK MEEHAN, Pennsylvania  
RICHARD L. HANNA, New York  
JEFFREY M. LANDRY, Louisiana  
STEVE SOUTHERLAND II, Florida  
JEFF DENHAM, California  
JAMES LANKFORD, Oklahoma  
REID J. RIBBLE, Wisconsin  
CHARLES J. "CHUCK" FLEISCHMANN,  
Tennessee

NICK J. RAHALL II, West Virginia  
PETER A. DeFAZIO, Oregon  
JERRY F. COSTELLO, Illinois  
ELEANOR HOLMES NORTON, District of  
Columbia  
JERROLD NADLER, New York  
CORRINE BROWN, Florida  
BOB FILNER, California  
EDDIE BERNICE JOHNSON, Texas  
ELIJAH E. CUMMINGS, Maryland  
LEONARD L. BOSWELL, Iowa  
TIM HOLDEN, Pennsylvania  
RICK LARSEN, Washington  
MICHAEL E. CAPUANO, Massachusetts  
TIMOTHY H. BISHOP, New York  
MICHAEL H. MICHAUD, Maine  
RUSS CARNAHAN, Missouri  
GRACE F. NAPOLITANO, California  
DANIEL LIPINSKI, Illinois  
MAZIE K. HIRONO, Hawaii  
JASON ALTMIRE, Pennsylvania  
TIMOTHY J. WALZ, Minnesota  
HEATH SHULER, North Carolina  
STEVE COHEN, Tennessee  
LAURA RICHARDSON, California  
ALBIO SIRES, New Jersey  
DONNA F. EDWARDS, Maryland



# CONTENTS

Hearing held on March 26, 2012 .....	Page 1
WITNESSES	
Mr. Christopher L. McLaughlin, Assistant Administrator for Security Operations, Transportation Security Administration	
Oral statement .....	5
Written statement .....	8
Mr. Stephen Sadler, Assistant Administrator for Intelligence and Analysis, Transportation Security Administration	
Oral statement .....	6
Written statement .....	8
Mr. Stephen M. Lord, Director, Homeland Security and Justice Issues, U.S. Government Accountability Office	
Oral statement .....	17
Written statement .....	00
Rear Admiral Paul F. Zukunft, Assistant Commandant for Marine Safety, Security, and Stewardship, U.S. Coast Guard	
Oral statement .....	19
APPENDIX	
The Honorable Elijah E. Cummings, a Member of Congress from the State of Maryland, Opening Statement .....	62
Facebook Questions & Comments for TSA .....	64
Questions for The Honorable John S. Pistole, Administrator, Transportation Security Administration from The Chairman of the Committee on Transportation and Infrastructure, The Honorable John L. Mica, a Member of Congress from the State of Florida .....	67
Submitted for the Record by The Honorable Blake Farenthold, a Member of Congress from the State of Texas .....	69
The Honorable Gerald E. Connolly, a Member of Congress from the State of Virginia, Opening Statement .....	70
Questions and Responses .....	71



## **TSA OVERSIGHT PART III: EFFECTIVE SECURITY OR SECURITY THEATER?**

**Monday, March 26, 2012**

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,  
JOINT WITH THE  
COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE,  
*Washington, D.C.*

The committees met, pursuant to call, at 1:32 p.m., in Room 2154, Rayburn House Office Building, Hon. Darrell E. Issa [chairman of the Committee on Oversight and Government Reform] presiding.

Present from the Committee on Oversight and Government Reform: Representatives Issa, Mica, Farenthold, Cummings, Norton, and Connolly.

Present from the Committee on Transportation and Infrastructure: Representatives Mica, Petri, Coble, Cravaack, Farenthold, Norton, Cummings, Boswell, and Cohen.

Also Present: Representative Blackburn.

Staff Present from the Committee on Oversight and Government Reform: Thomas A. Alexander, Senior Counsel; Michael R. Bebeau, Assistant Clerk; Molly Boyl, Parliamentarian; Gwen D'Luzansky, Assistant Clerk; Adam P. Fromm, Director of Member Services and Committee Operations; Linda Good, Chief Clerk; Mitchell S. Kominsky, Counsel; Mark D. Marin, Director of Oversight; Jeff Solsby, Senior Communications Advisor; Rebecca Watkins, Press Secretary; Kevin Corbin, Minority Deputy Clerk; Jennifer Hoffman, Minority Press Secretary; Carla Hultberg, Minority Chief Clerk; Peter Kenny, Minority Counsel; Lucinda Lessley, Minority Policy Director; and Carlos Uriarte, Minority Counsel.

Staff Present from the Committee on Transportation and Infrastructure: Gil Macklin, Professional Staff Member; Sean McMaster, Professional Staff Member; and Shant Boyajian, Professional Staff Member.

Chairman ISSA. The committee will come to order.

The Oversight Committee exists to secure two fundamental principles: First, Americans have a right to know that money Washington takes from them is well-spent; and, second, Americans deserve an efficient, effective government that works for them. Our duty on the Oversight and Government Reform Committee is to protect these rights.

Our solemn responsibility is to hold government accountable to taxpayers, because taxpayers have a right to know what they get from their government. We will work tirelessly, in partnership with

citizen watchdogs, to deliver the facts to the American people and bring genuine reform to the Federal bureaucracy.

This is our mission statement.

Today, we are calling the third hearing conducted by the Oversight Committee, today a joint hearing, where we plan to hold at least two additional TSA oversight hearings in April and May.

There is no question that the TSA serves a vital role. The question is, in a post-9/11 period, are we getting value for our money? Do we in fact have a system which is thorough and complete, that in fact takes care of all of us? Or do we have a fairly expensive, labor-intensive system that in fact is not making us appreciably safer? In a time of budget limitations, TSA, although essential, must in fact deliver value to the American people.

With more than 65,000 men and women working for TSA, it is not a small agency. This is more men and women working for an aviation-based safety organization than build all the Ford automobiles in America combined. Only one-quarter of the funds used by TSA come from aviation fees. Three-quarters come directly from the American people, meaning those of us who do not fly are paying a heavy price for those who do.

But even the billion-and-a-half-plus dollars paid for out of landing fees and other collections, ticket fees, to run our airports, in fact, is a high price to pay—a burden, if you will, on our efficiency. So whether the dollars come from ticket fees or come from the taxpayer directly, it is essential that we review TSA's effectiveness.

By 2013, TSA will arguably, by its own accounting, have wasted more than \$500 million of taxpayer money developing advanced imaging technology, or AIT, machines. In addition to public outrage over privacy violations, classified GAO reports paint a dire picture of ineffectiveness. GAO believes Screening of Passengers by Observation Techniques, or SPOT, program, which has already cost taxpayers \$800 million, is ineffective and that Congress should consider limiting funds for this program. GAO, as a nonpartisan organization, claims that TSA deployed SPOT before having solid scientific basis for its effectiveness and that when it worked, it was only an accident.

Despite a potential \$3.2 billion cost to the Federal Government and industry, GAO continues to find that TSA is failing to properly administer TWIC, the Transportation Worker Identification Credential. I have seen this failure myself. I have seen a mandated bio ID simply waived. Showing a picture ID is not, in fact, what Congress mandated. Deploying these and deploying them in a way in which they are quick and effective is essential. Let's remember, it cost a lot of money to produce the card; simply using it as a high-price ID card is not acceptable.

Without creating a plan to upgrade its explosive detection system, or EDS, which will cost \$964 million or more to the taxpayer, TSA cannot ensure updating EDS will be feasible or cost-effective. Now, let me just reiterate. EDS is an important system. Whether it is the inadvertent touching of fertilizer or the real operational use of explosives, we need to know. We need to screen. It is an effective tool if it works. If it doesn't work and work 100 percent of the time, we have the biggest problem we could possibly have.

Lastly, the VIPR program, Visual Intermodal Prevention and Response, faces serious questions from both security experts and legal scholars about the effectiveness and constitutionality of this initiative. TSA is not performing or taking into serious consideration the cost-benefits, and that is a big part of what this committee is here to ask questions on today. Not, is it nice to have; not, might it work; not, do we must do something; but, in fact, have we done a cost-benefit analysis? Have we screened through many choices, developed, researched, but only deployed those which work?

In fact, what we do know here at this committee and at the Transportation Committee is that we have fielded products that don't work, in the past. And when it becomes known by the public that a product has a gaping flaw, that product becomes essentially useless. Sadly, what we discover is, even when it becomes public, there is no other tool. So, in fact, we continue screening people, knowing that screening alone is not enough and that the public knows that.

And, with that, I now recognize the chairman of the Subcommittee on Aviation Infrastructure, Mr. Petri, for his opening statement.

Mr. PETRI. Thank you very much, Mr. Chairman. Thank you for organizing this important hearing and doing so with the Transportation Committee.

After 9/11, the Transportation Committee held a number of hearings to attempt to determine what happened and what needed to be done. And it became very clear at those hearings that the then-existing Federal policy of requiring easy access to the cockpit in case there was a medical emergency or something of that sort was not the most secure way to go. That policy was changed, and now our cockpits are hardened; that is to say, it is very difficult for a passenger to take over an airplane and turn it into a weapon, as happened on 9/11.

That, in my opinion, is the most significant security change since that time. Beyond that, of course, people can go on airplanes and possibly take a plane down, can create mischief, become a hara-kiri person, as they could if they were to go to a football stadium or on a cruise liner or any other sort of—a train—other modes of transportation. We do have a security problem, but it is not restricted to airlines. And the major part of the danger of airlines, I think, was dealt with when it became impossible for people to take over the airplane and turn it into a weapon, as happened on 9/11.

That said, of course, we have this regime that all of us experience who serve in Congress, if you live any distance at all, on a weekly basis practically, if not more often. We are inspecting millions of travelers, hundreds of thousands, every month, the same people over and over and over again. And that has to be wasteful and intrusive. And this has been going on now for 10 years. If it is going to go on for another 10 years, it behooves us to come up with a more efficient, less intrusive, more sensible program so that we concentrate on where there might be a risk, rather than inspecting the same people over and over and over again.

When we had hearings back at the time of 9/11, experts came in, testified before the Transportation Committee, from Israel and a number of other countries that certainly have for many years faced

very, very heightened security threats. Hardening the cockpit was one of the things that they advised and which we did. Other things that they have advised we have not done: trying to track people when they buy tickets and working on the intelligence side of things to see if there is some sort of a likelihood that that person might be a risk; put ways of inspecting people and how they behave not just at the airport, looking through their drawers and socks and looking at their shoes, but looking at how they interact with ticket agents, how they generally behave, not just at the airport but as they go about their business of preparing possibly to do things of risk.

It seems to me that there are a lot more strategic and intelligent ways to go about it than spending hundreds of millions of dollars, impeding the growth of the transportation sector, aviation sector, and basically changing the psychology of Americans to have them starting to feel that they somehow have done something wrong and they are being subjected to pat-down and shakedown, as we do when we are worrying about someone who has committed a crime or—we are assuming everyone is guilty and treating them practically like prisoners when they are American taxpaying citizens.

So I feel that we have a lot to do to straighten this whole mess out. It is not a cost-effective or very disciplined approach. And after 10 years, we owe more to the American people.

Mr. Chairman, thank you for having this hearing.

Chairman ISSA. I thank the gentleman.

Chairman ISSA. The gentleman yields back.

I now ask unanimous consent that our colleague from Tennessee, Mrs. Blackburn, be allowed to participate in today's hearing.

Without objection, so ordered.

I will now note that the ranking members of each of the committees are driving in and have been delayed. It is not a flight, as far as I know. So they will make their opening statements after our witnesses make theirs. I am assured they will be here by then.

With that, I would like to now introduce our first panel. Mr. Christopher L. McLaughlin is the Assistant Administrator for Security Operations at the Transportation Security Administration. Mr. Stephen Sadler is the Assistant Administrator for Intelligence and Analysis at the Transportation Security Administration. Mr. Stephen Lord is director for homeland security at the U.S. Government Accountability Office—our wing, if you will. And Rear Admiral Zukunft, with the U.S. Coast Guard, is an Assistant Commandant for Marine Safety, Security, and Stewardship, and I might mention, without a doubt the best jewel ever given to homeland security, in my opinion and in the ranking member's opinion.

Pursuant to the rules of this committee, would you all please rise to take the oath? Raise your right hand.

Do you solemnly swear or affirm that the testimony you are about to give will be the truth, the whole truth, and nothing but the truth?

Let the record indicate that—please have a seat—all witnesses answered in the affirmative.

Now, my predecessor, whose portrait is up there, Mr. Towns, began a tradition of explaining the obvious, but he did it every time, and I appreciated it. Your entire opening statements will be

placed in the record. In front of you you have a countdown clock. And like so many things that you look at, you say, does it really matter? The answer is, please summarize if you run out of time. We would like to get through all of you and get you out of here with full questions and answers in a timely fashion. And remember, your opening statements will be available in their entirety.

Mr. McLaughlin, you are first. You have 5 minutes.

## **WITNESS STATEMENTS**

### **STATEMENT OF CHRISTOPHER L. MCLAUGHLIN**

Mr. MCLAUGHLIN. Good afternoon, Chairman Issa and distinguished members of the committees. Thank you for the opportunity to testify today.

TSA has made significant strides in our deployment and utilization of AIT over the past year. Automatic Target Recognition software, recently installed in the majority of our machines, enhanced passenger privacy by eliminating passenger-specific images, while improving throughput capabilities and streamlining the checkpoint screening process.

In the fall of 2011, my office began to further develop operational performance targets, including a new AIT utilization goal that is consistent with the DHS, OIG, and GAO recommendations. Tied to this, we implemented an action plan to increase AIT utilization across the Nation. As a result of these efforts, our utilization performance between February 2011 and February 2012 improved by 200 percent.

In addition to AIT, we are employing CAT/BPSS technology to automatically verify passenger documents. CAT/BPSS will eventually replace the current procedures used to detect fraudulent or altered documents. We will deploy this technology for operational testing at a few airports beginning next month.

Technology is only one mechanism to identify potential threats. The SPOT program uses behavior observation and analysis to identify potentially high-risk individuals who may pose a threat to transportation security. SPOT was scientifically validated in 2011 by the DHS Science and Technology Division, representing the most thorough analysis of any behavioral screening program to date. No other counterterrorism or similar security program is known to have been subjected to such a rigorous, systematic evaluation. This study revealed that SPOT was significantly more effective at identifying high-risk passengers than random screening protocols. That said, TSA continues working with DHS S&T and the broader research community to increase the effectiveness and the efficiency of this behavior-based screening process.

Subsequent to the validation study, TSA took steps last fall to enhance the program. Under a new pilot, behavior detection officers employ a specialized interview technique to determine if a traveller should be referred for additional screening at the checkpoint. This additional interaction, used by security agencies worldwide, enables officers to better verify or dispel concerns about suspicious behavior and anomalies. Preliminary analysis shows an increase in the rate of detection of high-risk passengers. And TSA is

currently conducting analysis with the DHS Science and Technology Directorate to inform a validation process for future rollout.

Complementing these program developments, TSA has begun teaching a tactical communications course for our frontline workforce. This training focuses on active listening, empathy, and verbal communication techniques and will be complete by the end of 2012.

These initiatives are some of the key aspects of TSA's security infrastructure that provide the backbone for our overall risk-based strategy. This strategy demonstrates our commitment to move away from a one-size-fits-all security model. While this approach was necessary after 9/11 and has been effective over the past decade, key enablers now allow TSA to move toward a more intuitive solution.

Perhaps the most widely known RBS initiative is TSA PreCheck. To date, approximately 600,000 passengers have experienced an expedited screening through TSA PreCheck. By the end of 2012, we expect to offer to passengers in 35 of our busiest airports the benefits of TSA PreCheck. In addition to eligible frequent fliers and members of CBP's Trusted Traveler programs, we just expanded PreCheck to include active-duty U.S. military traveling out of Reagan National Airport.

In addition to PreCheck, last fall we implemented new screening procedures for children 12 and under, allowing them to leave their shoes on and go through a less intrusive security screening process. And just last Monday, at a few airports we began testing similar modified procedures for passengers 75 and older.

Finally, we are also supporting efforts to test identity-based screening for airline pilots. So far, over 470,000 uniformed pilots have cleared security through the Known Crewmember program.

These initiatives have allowed us to expedite the screening process for children, our military, many frequent fliers, and, now in testing, the elderly. They have resulted in fewer divestiture requirements and a significant reduction in pat-downs, while allowing us more time to focus on travelers we believe are likely to pose a risk to our transportation network, including those on terrorist watchlists.

By enhancing the effectiveness of our current programs and layering in our risk-based security initiatives, TSA continues to work toward our goal of providing the most effective security in the most efficient way.

Thank you again for the opportunity to testify.

At this time, I would like to introduce my colleague, Mr. Stephen Sadler, Assistant Administrator for TSA's Office of Intelligence and Analysis.

Chairman ISSA. The gentleman is recognized.

#### **STATEMENT OF STEPHEN SADLER**

Mr. SADLER. Good afternoon, Chairman Issa and distinguished members of the committees. I appreciate the opportunity to testify on some of the work we are doing in coordination with the United States Coast Guard to strengthen security throughout our Nation's maritime transportation system.

The Transportation Worker Identification Credential program, or TWIC, is an important security measure designed to ensure that

individuals who pose a threat to security do not gain unescorted access to secure areas of certain maritime facilities and vessels. Prior to the TWIC program, there was no standard identity verification or background check policy for entrance to a port. Today, facility owners and operators can look for one standard identification document issued after the successful completion of a thorough security threat assessment.

The identity verification and threat assessment requirements of the TWIC program support the DHS multilayered approach to protecting the Nation's transportation system and enhance security at our ports. Several key objectives, included in the SAFE Port Act of 2006, were met during the initial rollout of the program in October 2007. These include milestones for implementing TWIC enrollment sites, conducting security threat assessments, and issuing TWICs.

On April 15, 2009, U.S. Coast Guard regulation implemented the requirement for all unescorted workers in secure areas and all mariners to possess a valid TWIC. As of this month, almost 2 million transportation workers, including longshoremen, truckers, and port employees, have received a TWIC.

This past February, TSA deployed changes to allow TWIC holders to receive comparability for the security threat assessment when applying for a hazardous materials endorsement under a State-issued commercial driver's license. Under comparability, hazmat applicants with a valid TWIC can pay a reduced fee and do not need to go to an enrollment center; they can go directly to their State licensing agency to apply for this endorsement. Currently, 11 States and the District of Columbia have availed themselves of this capability.

TSA also recently awarded its Universal Enrollment Services contract. This new capability will allow individuals to apply for multiple programs such as TWIC and HME at the same location, provide enrollment centers across a broader geographic range, and allow enrollment for new or future programs serviced by TSA.

On May 31st, 2011, TSA completed the required data collection phase of the TWIC Reader Pilot. TSA gathered information from 7 ports, 13 facilities, and 4 vessel operations that collectively installed 156 readers of various types and models best suited to their business needs. These sites provided data regarding reader performance and reliability as well as throughput data of vehicle and pedestrian access points.

The final report was submitted to Congress February 27th, 2012. This data provides a clearer picture of the likely impacts of using readers at maritime facilities and on vessel operations. The TWIC Reader Pilot concludes that TWIC reader systems function properly when they are designed, installed, and operated in a manner consistent with the characteristics and business needs of the facility or the vessel operation.

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

Chairman ISSA. Thank you.

[Prepared statement of Mr. McLaughlin and Mr. Sadler follows.]

**Statement of**  
**Chris McLaughlin**  
**Assistant Administrator, Security Operations**  
**Transportation Security Administration**  
**U.S. Department of Homeland Security**  
**and**  
**Stephen Sadler**  
**Assistant Administrator for Intelligence and Analysis**  
**Transportation Security Administration**  
**U.S. Department of Homeland Security**  
**Before the**  
**United States House of Representatives**  
**Committee on Oversight and Government Reform**  
**and**  
**Committee on Transportation and Infrastructure**  
**March 26, 2012**

Good afternoon Chairman Issa, Chairman Mica, Ranking Member Cummings and Ranking Member Rahall, and distinguished Members of the Committees. Thank you for the opportunity to testify today about the Transportation Security Administration's (TSA) successes and challenges in developing and implementing a comprehensive risk-based approach to secure our Nation's transportation systems.

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 protects the Nation's transportation systems to ensure freedom of movement for people and commerce. TSA's security measures create a multi-layered system of transportation security that mitigates risk. We continue to evolve our security approach by examining the procedures and

technologies we use, how specific security procedures are carried out, and how screening is conducted.

#### Risk-Based Security Improves the Travel Experience

Last Fall, TSA began developing a strategy for enhanced use of intelligence and other information to enable more risk-based security (RBS) in all facets of transportation, including passenger screening, air cargo, and surface transportation. At its core, the concept of RBS demonstrates a progression of the work TSA has been doing throughout its first decade of service to the American people. RBS is an acknowledgment that risk is inherent in virtually everything we do. Our objective is to mitigate risk in a way that effectively balances security measures with privacy and civil liberty concerns while both promoting the safe movement of people and commerce and guarding against a deliberate attack against our transportation systems.

RBS in the passenger screening context allows our dedicated Transportation Security Officers (TSOs) to focus more attention on those travelers we believe are more likely to pose a risk to our transportation network – including those on terrorist watch lists – while providing expedited screening, and perhaps a better travel experience, to those we consider pose less risk.

Through various RBS initiatives, TSA is moving away from a one-size-fits-all security model and closer to its goal of providing the most effective transportation security in the most efficient way possible. While a one-size-fits-all approach has been effective over the past decade, two key enablers – technology and intelligence – are allowing TSA to move toward a RBS model.

#### TSA Pre✓™ Program

Perhaps the most widely known risk-based security enhancement we are putting in place is TSA Pre✓™. Since first implementing this idea last Fall, the program has been expanded to twelve airports and over 500,000 passengers around the country have experienced expedited security screening through TSA Pre✓™. The feedback we've received is consistently positive.

Under TSA Pre✓™, travelers volunteer information about themselves prior to flying.

By changing procedures for those travelers we know more about, through information they voluntarily provide, and combining that information with our multi-layered system of aviation security, TSA can better focus our limited resources on higher-risk and unknown passengers. This new screening system holds great potential to strengthen security while significantly enhancing the travel experience, whenever possible, for passengers.

TSA pre-screens TSA Pre✓™ passengers each time they fly through participating airports. If the indicator embedded in their boarding pass reflects eligibility for expedited screening, the passenger is able to use the Pre✓™ lane. Currently, eligible participants include certain frequent flyers from American Airlines and Delta Air Lines as well as existing members of U.S. Customs and Border Protection's (CBP) trusted traveler programs, such as Global Entry, who are U.S. citizens and are flying domestically on participating airlines. TSA is actively working with other major air carriers such as United Airlines, US Airways, Jet Blue, Hawaiian Airlines, and Alaska Airlines to expand both the number of participating airlines and the number of airports where expedited screening through TSA Pre✓™ is provided. In February 2012, Secretary Napolitano and TSA Administrator Pistole announced the goal to have TSA Pre✓™ rolled out and operating at 35 of the busiest domestic airports by the end of 2012.

TSA Pre✓™ travelers are able to divest fewer items, which may include leaving on their shoes, jacket, and light outerwear, and may enjoy other modifications to the standard screening process. As always, TSA will continue to incorporate random and unpredictable security measures throughout the security process. At no point are TSA Pre✓™ travelers guaranteed expedited screening.

Earlier this month, we expanded the TSA Pre✓™ population to include active duty U.S. Armed Forces members with a Common Access Card (CAC) traveling out of Ronald Reagan Washington National Airport. Service members will undergo the standard TSA Secure Flight pre-screening and if we are able to verify the service member is in good standing with the Department of Defense, by scanning their CAC card at the airport, they will receive TSA Pre✓™ screening benefits, such as no longer removing their shoes or light jacket and allowing them to keep their laptop in its case and their 3-1-1 compliant bag in a carry-on.

In addition to active duty members of the United States Army, Navy, Air Force, Marine Corps and Coast Guard, this evaluation will also include active drilling members of the U.S. National Guard and reservists. U.S. service members are entrusted to protect and defend our Nation and its citizens with their lives. In treating them as trusted travelers, TSA is recognizing that these members pose little risk to aviation security. This evaluation is being conducted in compliance with the "Risk-Based Security Screening for Members of the Armed Forces Act," signed into law by the President on January 3, 2012. (Pub. L. No. 112-86.)

#### Streamlining the Process for Inbound International Passengers

TSA Pre✓™ is being extended to any U.S. citizen who is a member of one of the trusted traveler programs operated by CBP.

To further expedite the screening process, CBP currently operates 14 international aviation preclearance locations. Each of these locations has been or is scheduled to be evaluated by TSA to confirm that preclearance airports are performing checkpoint screening procedures of passengers and accessible property comparable to those of domestic airports and are providing an equivalent level of protection. All precleared flights arriving from the 14 preclearance airports are permitted to deplane passengers directly into the sterile area of U.S. airports. Connecting passengers' checked baggage intended for connecting domestic flights must still be screened by TSA upon arrival in the United States, until the screening technology and protocols at the preclearance airports are comparable to TSA domestic checked baggage requirements.

In addition, under the Beyond the Borders (BTB) initiative, in accordance with a joint declaration signed by President Obama and Canadian Prime Minister Stephen Harper on February 4, 2011, TSA has been working with Transport Canada (TC) towards mutual recognition of the two countries' checked baggage screening systems. Canada's eight preclearance airports (Calgary, Edmonton, Halifax, Montréal, Ottawa, Toronto, Vancouver, and Winnipeg) have initiated the process to deploy TSA-certified explosives detection system (EDS) equipment as the primary checked baggage screening equipment. The deployment of TSA-certified EDS partnered with comparable implementation of TSA policies and procedures will make it unnecessary to rescreen checked bags from these Canadian airports when the passengers

connect in the United States to other flights.

AIT is a Critical Component of RBS

Advanced Imaging Technology (AIT) is a critical component of TSA's multi-layered system of transportation security that mitigates risk, facilitates the flow of legitimate commerce and protects individual privacy. Consistent with recent Department of Homeland Security (DHS) Office of Inspector General and Government Accountability Office recommendations, TSA is implementing an action plan to increase the level of available AIT screening capacity across the nation's aviation system. Where AIT is deployed and relied upon, TSA has established a utilization target consistent with the recommendation by OIG, and is meeting or exceeding that target.

Based upon recommendations in the audits, TSA has revised training and staffing availability to operate the equipment and resolve anomalies. TSA developed and implemented an AIT instructor certification curriculum for Security Training Instructors (STI) assigned at the airports. These STIs are responsible for delivering AIT training as airports receive the technology. A full training curriculum package, including training kits and training aids, has been distributed to all AIT airports and allows each airport to train as many operators as required. Airports that have not received AIT units will receive the training kit and aids when the equipment is installed. In addition, introduction of Automated Target Recognition (ATR) functionality eliminated the need for a remote Image Operator in all new machines, and in all existing machines using millimeter-wave technology. As a result of this reduced training length and certification of local STIs, TSA does not consider training to be a constraint in achieving our AIT utilization goal.

In support of the increasing number of AIT units deployed with ATR, TSA is developing a new training kit specifically designed to support AIT ATR training and testing. TSA is also working to increase the number of AIT testing scenarios for the Aviation Screening Assessment Program (ASAP) from 6 to 10. In coordination with the Johns Hopkins University Applied Physics Laboratory, TSA has been conducting a preliminary assessment to develop and validate additional testing stimulants and scenarios for use with the AIT ATR equipment. The intent is to

incorporate new scenarios and stimulants appropriate for use with AIT ATR into ASAP's national level testing framework.

TSA has begun rolling out a Tactical Communications course for its front line workforce which is designed to specifically help them develop their communications skills. Training for all airport Supervisors and Security Managers is on target to be completed by June 2012, and all officers must complete the training by December 2012.

These advancements are representative of the types of improvements that have resulted from TSA's desire to improve the AIT program and openness to outside recommendations regarding it.

#### TWIC Secures Maritime Transportation System

The Transportation Worker Identification Credential (TWIC) is an important security measure to ensure that individuals who pose a security threat do not gain unescorted access to secure areas of the Nation's maritime transportation system. Prior to the TWIC program, there was no standard identity verification or background check policy for entrance to a port, which created opportunities for fraud and risk. Today, facility owner/operators have one standard identification document to look for that confirms the holder's identity, and verifies that he or she successfully passed a thorough security threat assessment. TWIC cards contain security features that make the card highly resistant to counterfeiting and difficult to use by anyone other than the authorized holder. When biometric verification becomes a requirement and readers are in widespread use, we will enhance security at the ports even further.

The TWIC program is a fee-funded, joint effort of TSA and the United States Coast Guard (USCG). TSA establishes TWIC enrollment sites, conducts identity verification and risk-based security threat assessments (STAs), and provides a tamper-resistant biometric credential to eligible maritime workers requiring unescorted access to secure areas of port facilities and vessels regulated under the Maritime Transportation Security Act of 2002 (MTSA), Pub. L. No. 107-295. The USCG regulates facility and vessel security standards, approves security plans, and conducts enforcement.

In the Coast Guard Authorization Act of 2010, Pub. L. No. 111-281, Congress limited the applicability of the transportation security card to those mariners who were allowed unescorted access to a secure area designated in a vessel security plan (46 U.S.C. § 70105). The identity verification and threat assessment requirements of the TWIC program support DHS's multi-layered approach to protecting the nation's transportation systems and significantly enhance security at ports across the Nation. Over two million workers including longshoremen, truckers, port employees and others have applied to obtain a TWIC as of March 2012.

The SAFE Port Act of 2006, Pub. L. No. 109-347, milestones for implementing the TWIC enrollment sites, conducting STAs, and issuing TWICs were met during the October 2007 to April 2009 initial rollout of the program. On April 15, 2009, the requirement for all unescorted workers in secure areas and all mariners to possess a valid TWIC was implemented nationwide by USCG regulation. Since April 2009, TSA has enrolled approximately 25,000 workers per month. On October 20, 2011, TSA enrolled the program's two millionth worker.

On May 31, 2011, TSA completed the data collection phase of the TWIC reader pilot program that was required by Section 104 of the SAFE Port Act and Section 802 of the Coast Guard Authorization Act of 2010. During this period, data was gathered from pilot sites including ports, facilities, and vessel operations regarding reader performance and reliability as well as throughput data at vehicle and pedestrian access points, which is critical to evaluating the impact of reader use on facility and vessel operations.

TSA completed the final analysis of data collected from participating ports, facilities, and vessel operations and drafted a final report which was approved by the Secretary of Homeland Security and transmitted to Congress on February 27, 2012. The TWIC Reader Pilot report found that while the operational and technological difficulties were wide-ranging, the Reader Pilot successfully examined the impacts to business. Although current infrastructure was key to installation costs and time, the Reader Pilot also noted that reader performance varied widely and there were problems with the durability of the card stock and ability of the cards to be read by the various readers that were used throughout the pilot. TSA will publish lessons learned from the pilot to assist ports and facility operators with their reader and reader system decisions. The submission of the TWIC Reader Pilot report completed all actions required by TSA under the

SAFE Port Act. The USCG is responsible for the TWIC reader regulation. A Notice of Proposed Rulemaking will be published to obtain stakeholder feedback, followed by the final rule.

SPOT Adds Additional Mobile Layer of Security

In addition to relying upon the best available technology to enable TSA to identify potential threats to the Nation's transportation system, the Screening of Passengers by Observation Techniques (SPOT) program uses behavior observation and analysis to identify potentially high-risk individuals who may pose a threat to transportation security. This is accomplished by detecting behaviors and activities that deviate from an established environmental baseline. Individuals whose behaviors meet or exceed predetermined thresholds are referred for additional screening or law enforcement intervention.

Since its inception in 2004, SPOT has proven to be an effective mobile layer of security. To date, 331,258 SPOT referrals have resulted in 27,342 Law Enforcement referrals which led to the arrest of more than 2,273 individuals for various reasons such as fraudulent documents, narcotics trafficking, outstanding warrants, and immigration violations. At the current time, TSA is authorized to deploy over 3,100 behavior detection officers at over 170 airports.

SPOT is a scientifically validated behavior-based security program. In April 2011, the DHS Science & Technology (S&T) Division completed a research study that examined the extent to which SPOT indicators led to correct screening decisions at the security checkpoint. The study revealed that SPOT was significantly more effective at identifying High Risk Passengers (HRP) than random selection protocols. This study represents the most thorough analysis of any behavioral screening program to date; no other counter-terrorism or similar security program is known to have been subjected to such a rigorous, systematic evaluation of its screening accuracy.

TSA continues to work with DHS S&T and the broader research community to define and prioritize the research required to further increase the effectiveness and efficiency of TSA's behavior-based screening process. This continued emphasis on research includes the collection of operational video to support a number of research studies to include fatigue, reliability, and indicator refinement.

TSA is exploring the use of enhanced behavior detection to identify risk. Through the Assessor Proof of Concept (PoC) at Boston Logan International Airport (BOS) and Detroit Metropolitan Wayne County Airport (DTW), TSA is testing the ability of “Assessors” to perform real-time risk assessments through engagement and observation at the screening checkpoint. The current concept of operations (CONOPS) requires Assessors to perform document review and interviews with all transiting passengers, while observing for suspicious signs and behavioral anomalies. Based on the results of this engagement and observation, Assessors direct passengers to either standard or secondary screening.

TSA is collecting data that is consistent with the SPOT Validation study to evaluate the effect of this pilot on both TSA efficiencies and security effectiveness. The goal of this pilot is to develop behavior detection procedures that enhance security from its current level while maintaining program efficiencies and improving passenger satisfaction. Preliminary data from the pilots reveal an improvement in security posture over a baseline period.

#### Conclusion

Thank you for the opportunity to appear before you today to discuss the successes and challenges facing TSA in developing and implementing a comprehensive risk-based approach to secure our Nation’s transportation systems.

Chairman ISSA. Mr. Lord?

**STATEMENT OF STEPHEN M. LORD**

Mr. LORD. Thank you, Mr. Chairman and other members of the committee. Thank you for inviting me here today to discuss TSA's progress and related challenges in deploying three key security programs. My observations are based on a large body of work the GAO has completed over the last few years.

I would first like to note that DHS and TSA have made some notable achievements since the 9/11 attacks in securing our Nation's ports and airports. And as the TSA witnesses noted today, some remaining challenges still exist.

The first program I would like to discuss today is TSA's behavior detection program, also called SPOT. This program consists of over 3,000 behavior detection officers that are deployed to over 160 U.S. airports. This program is a key part of TSA's efforts to focus more attention on dangerous people versus dangerous items, which I support.

Bottom line on the program is, while TSA has taken some steps to validate the science behind the program, much more work remains to fully validate it, establish sound performance metrics, and assess costs and benefits. And as we noted in our prior work, all these additional steps could take several more years to complete.

And as we noted in our report on the program, TSA deployed SPOT nationwide before determining whether it had a valid scientific basis. The good news is, DHS did complete an initial validation study in April 2011, which concluded that the program was more effective than random screening. However, as the study itself noted, it was not designed to fully answer the very important question of whether you can use behavior detection principles for counterterrorism purposes in the airport environment. A scientific consensus on this issue simply does not exist.

Another key report recommendation was to develop better performance measures. The importance of this is underscored by looking at the arrests made under the program. For example, 27 percent of the 300 SPOT arrests made in 2010 were illegal aliens, raising questions about mission focus.

The second TSA program I would like to discuss today is TSA's body scanner program, commonly referred to as advanced imaging technology or AITs. As you know, these scanners were deployed in response to the attempted Christmas Day attack of a Northwest Airlines flight. About 640 of these units are now in place at over 160 airports. According to TSA, these machines provide superior benefits over walk-through metal detectors since they are capable of detecting non-metallic threat objects.

Earlier this year, we issued a classified report on AIT. While most of the details are still classified, TSA agreed to allow us to note some of the details regarding the utilization rates of these units for today's hearing. We found that some of these units had been used less than 30 percent of the day since their installation. And the good news is, in response to our report, TSA agreed to take steps to address these low utilization rates.

The last program I would like to briefly discuss today is TSA's maritime biometric credential program called TWIC. In terms of

progress, TSA has now enrolled over two million maritime workers in the program. However, our 2011 report identified a number of significant internal control weaknesses in card enrollment, background checking, and use that we believe have limited the security benefits of the program. In fact, these weaknesses may have contributed to the breach of selected U.S. facilities during covert tests we conducted as part of this review.

We recommended that DHS and TSA strengthen program controls as well as complete an effectiveness study to clarify the current program's contributions to enhancing maritime security. DHS has established a working group with executive oversight to address our important TWIC report recommendations. We look forward to seeing the results of this committee's work.

In closing, TSA has established a number of security layers and programs to thwart potential terrorist attacks. However, our past work has identified a number of ways these efforts could be strengthened to help ensure American taxpayers receive a good return on their considerable investment. I am hoping that today's hearing can provide some additional insights on how these programs can be strengthened and be made more cost-effective.

Mr. Chairman, this concludes my statement, and I look forward to your questions.

Chairman ISSA. Thank you.

[Prepared statement of Mr. Lord follows.]

United States Government Accountability Office

---

**GAO**

Testimony  
Before the Committee on Oversight and  
Government Reform and Committee on  
Transportation and Infrastructure, House  
of Representatives

---

For Release on Delivery  
Expected at 1:30 p.m. EDT  
Monday, March 26, 2012

**TRANSPORTATION  
SECURITY  
ADMINISTRATION**

**Progress and Challenges  
Faced in Strengthening  
Three Key Security  
Programs**

Statement of Stephen M. Lord, Director  
Homeland Security and Justice Issues





Highlights of GAO-12-541T, a testimony before the Committee on Oversight and Government Reform and Committee on Transportation and Infrastructure, House of Representatives

### Why GAO Did This Study

DHS and TSA have made some notable achievements in securing the nation's transportation systems since the terrorist attacks of September 11, 2001, but in recent years, GAO reported that DHS has experienced challenges in managing its efforts including fielding programs prior to determining their effectiveness or completing cost-benefit analyses. This testimony focuses on, among other things, DHS and TSA's progress and challenges in implementing three key security programs: SPOT, AIT, and TWIC. This testimony is based on reports and testimonies issued from November 2009 through March 2012, and includes selected updates conducted from February through March 2012. To conduct these updates, GAO obtained information on the current status of the programs and progress made related to the implementation of recommendations contained in prior GAO reports.

### What GAO Recommends

GAO is not making any new recommendations. In prior work, GAO made recommendations to address challenges related to assessing SPOT effectiveness as well as AIT utilization. GAO also recommended that DHS assess TWIC effectiveness and use this assessment to evaluate the costs, benefits, and risks of TWIC. DHS and TSA concurred and have actions underway to address the recommendations.

View GAO-12-541T. For more information, contact Steve Lord at (202) 512-4379 or lords@gao.gov.

March 26, 2012

## TRANSPORTATION SECURITY ADMINISTRATION

### Progress and Challenges Faced in Strengthening Three Key Security Programs

#### What GAO Found

The Transportation Security Administration (TSA) relies on layers of security encompassing personnel, processes, and technology to deter, detect, and disrupt persons posing a potential risk to aviation security. The Screening of Passengers by Observation Techniques (SPOT) program consists of about 3,000 behavior detection officers (BDO) who examine passengers to identify those who might pose a security risk at over 160 TSA-regulated airports. Advanced Imaging Technology (AIT)—full body scanners—are intended to help TSA staff detect explosives and other threats on passengers. Also, TSA and the U.S. Coast Guard manage the Transportation Worker Identification Credential (TWIC) program, which employs a federally-sponsored credential in an effort to enhance access controls at Maritime Transportation Security Act regulated facilities and vessels. The Department of Homeland Security (DHS) and TSA have made progress and faced challenges in implementing these programs.

**SPOT.** Additional DHS and TSA actions are needed to validate SPOT and to establish performance measures. GAO reported in May 2010 that TSA deployed SPOT nationwide before determining whether it had a scientifically valid basis. GAO recommended that DHS convene an independent panel of experts to review DHS's efforts to validate SPOT and determine whether the methodology used was sufficiently comprehensive. DHS agreed and completed this study in April 2011. The study found that SPOT was more effective than random screening to varying degrees; however, as noted in the study, the assessment was an initial validation step and was not designed to fully validate whether BDOs can reliably identify individuals who pose a security risk. According to DHS, additional work will be needed to validate SPOT. Also, GAO reported that TSA has implemented certain performance measures to assess the program, but has not fielded outcome-oriented performance measures—which track progress by documenting the beneficial results of programs—to help assess SPOT's contribution to improving aviation security. In May 2010, GAO recommended and TSA agreed that to better measure SPOT's effectiveness and evaluate the performance of BDOs, TSA should establish a plan to develop outcome-oriented performance measures.

**AIT.** DHS accelerated the deployment of AIT to identify threat materials and to provide enhanced security benefits compared to metal detectors. In January 2012, GAO reported instances where AIT units were not being used, raising questions about the cost-effectiveness of this acquisition. For example, data GAO collected from March 2010 through February 2011 on all deployed AIT units showed that some deployed units were not used regularly, decreasing their potential security benefit. GAO recommended and TSA agreed to study AIT utilization and address the extent to which currently deployed units are used.

**TWIC.** As of March 2012, the TWIC program has enrolled over 2.1 million maritime workers and DHS has established TWIC-related processes and controls. In May 2011, GAO recommended that DHS conduct an assessment that includes addressing internal control weaknesses and evaluate whether use of TWIC would further enhance the security posture. GAO also recommended that this assessment be used to evaluate the costs, benefits, and security risks of the TWIC program prior to requiring its use. DHS agreed and, as of March 2012, reports that it is further evaluating the TWIC program.

---

Chairmen Issa and Mica, Ranking Members Cummings and Rahall, and Members of the Committees:

I am pleased to be here today to discuss our past work examining the Transportation Security Administration's (TSA) progress and challenges in improving transportation security. Securing commercial aviation operations remain a daunting task—with hundreds of airports, thousands of aircraft, and thousands of flights daily carrying millions of passengers and pieces of checked baggage. The attempted terrorist bombing of Northwest flight 253 on December 25, 2009, provided a vivid reminder that civil aviation remains an attractive terrorist target and underscores the need for effective passenger screening. Likewise, securing operations at our nation's maritime ports requires balancing security to address potential threats while facilitating the flow of people and goods that are critical to the U.S. economy and international commerce. Transportation systems and facilities are vulnerable and difficult to secure given their size, easy accessibility, large number of potential targets, and proximity to urban areas.

As noted in our 9/11 Anniversary report, the terrorist attacks of September 11, 2001, led to profound changes in government agendas, policies, and structures to confront homeland security threats facing the nation.<sup>1</sup> As highlighted in this report, the Department of Homeland Security (DHS) and TSA have made notable achievements since these attacks, including developing programs and technologies to screen passengers, and control access to secured airport areas and port facilities, yet challenges remain.

My testimony today focuses on DHS and TSA's progress and related challenges in implementing three key programs:

- Screening of Passengers by Observation Techniques (SPOT) program—A TSA-designed program to provide behavior detection officers (BDO) with a means of identifying persons who may pose a potential security risk at TSA-regulated airports by focusing on behaviors and appearances that deviate from an established baseline and that may be indicative of stress, fear, or deception.

---

<sup>1</sup> GAO, *Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11*, GAO-11-881 (Washington, D.C.: Sept. 7, 2011).

- 
- Advanced Imaging Technology (AIT)—a technology used to screen passengers in the nation's airports.
  - Transportation Worker Identification Credential (TWIC) program—a DHS program that requires maritime workers to complete background checks and obtain a biometric identification card to gain unescorted access to secure areas of regulated maritime facilities.

This statement is based on our reports and testimonies issued from March 2010 through March 2012 related to TSA's efforts to manage transportation security programs as well as selected updates, conducted from February 2012 through March 2012, related to the current status of the SPOT and TWIC programs and progress made on implementing previous GAO recommendations aimed at correcting program deficiencies.<sup>2</sup> For our past work, we reviewed applicable laws, regulations, and policies. We also conducted interviews with DHS component program managers and Science and Technology Directorate officials to discuss issues related to individual programs, visited selected airports to observe operations and meet with key program personnel, analyzed available data from relevant program databases, and used other methodologies. As part of our TWIC work, our investigators conducted covert testing at enrollment center(s) to identify whether individuals providing fraudulent information could acquire an authentic TWIC, and at maritime ports with facilities regulated pursuant to the Maritime Transportation Security Act of 2002 (MTSA) to identify security vulnerabilities and program control deficiencies. More detailed information on the scope and methodology from our previous work can be found within each specific report. For the updates, we obtained budget information from TSA and information on its efforts to conduct a cost-benefit analysis of the SPOT program, as well as efforts to address TWIC program internal control weaknesses, among other things. We conducted this work in accordance with generally accepted government auditing

---

<sup>2</sup> We are evaluating the results of a TWIC pilot and the DHS report on the results of the TWIC pilot that was submitted to the House Committees on Homeland Security and Transportation and Infrastructure and the Senate Committees on Commerce, Science, and Transportation and Homeland Security and Governmental Affairs, as well as to the Comptroller General, on February 27, 2012 pursuant to section 802 of the Coast Guard Authorization Act of 2010. See Pub. L. No. 111-281, 124 Stat. 2905, 2989-90 (2010). We plan to issue a report with the results from this work by the end of 2012. At the request of the House Committee on Transportation and Infrastructure we are initiating a review of the SPOT program which will examine TSA efforts to address some of the limitations identified in earlier DHS and GAO studies. We plan to issue a report with the results from this work in 2013.

---

standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We conducted our related investigative work in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

---

## Background

The Aviation and Transportation Security Act (ATSA) established TSA as the federal agency with primary responsibility for securing the nation's civil aviation system, which includes the screening of all passengers and property transported from and within the United States by commercial passenger aircraft.<sup>3</sup> In accordance with ATSA, all passengers, their accessible property, and their checked baggage are screened pursuant to TSA-established procedures at the 446 airports presently regulated for security by TSA. These procedures generally provide, among other things, that passengers pass through security checkpoints where they and their identification documents, and accessible property, are checked by transportation security officers (TSO), other TSA employees, or by private-sector screeners under TSA's Screening Partnership Program.<sup>4</sup> Airport operators, however, also have direct responsibility for implementing TSA security requirements, such as those relating to perimeter security and access controls, in accordance with their approved security programs and other TSA direction.

TSA relies upon multiple layers of security to deter, detect, and disrupt persons posing a potential risk to aviation security. These layers include BDOs, who examine airport passenger behaviors and appearances to identify passengers who might pose a potential security risk at TSA-regulated airports; travel document checkers, who examine tickets, passports, and other forms of identification; TSOs responsible for screening passengers and their carry-on baggage at passenger

---

<sup>3</sup> See Pub. L. No. 107-71, 115 Stat. 597 (2001). For purposes of this testimony, "commercial passenger aircraft" refers to U.S. or foreign-flagged air carriers operating under TSA-approved security programs with regularly scheduled passenger operations to or from a U.S. airport.

<sup>4</sup> Private-sector screeners, employed by an entity under contract to and overseen by TSA, and not TSOs, perform screening activities at the 16 airports currently participating in TSA's Screening Partnership Program as of March 2012. See 49 U.S.C. § 44920.

---

checkpoints, using X-ray equipment, magnetometers, AIT, and other devices; random employee screening; and checked-baggage screening.<sup>5</sup>

MTSA required the Secretary of Homeland Security to prescribe regulations preventing individuals from having unescorted access to secure areas of MTSA-regulated facilities and vessels unless they possess a biometric transportation security card<sup>6</sup> and are authorized to be in such an area.<sup>7</sup> Pursuant to MTSA, the Secretary shall issue such biometric transportation security cards to eligible individuals unless the Secretary determines that an applicant poses a security risk warranting denial of the card. The TWIC program is designed to implement these biometric maritime security card requirements. The program requires maritime workers to complete background checks to obtain a biometric identification card and be authorized to be in the secure area by the owner/operator in order to gain unescorted access to secure areas of MTSA-regulated facilities and vessels. Within DHS, TSA and the U.S. Coast Guard manage the TWIC program.

A federal regulation (known as the credential rule) issued in January 2007 sets a compliance deadline, subsequently extended to April 15, 2009, whereby each maritime worker would be required to hold a TWIC in order to obtain unescorted access to secure areas of MTSA-regulated facilities and vessels.<sup>8</sup> A second rule, the card reader rule, is currently under development and is expected to address how the access-control technologies, such as biometric card readers, are to be used for confirming the identity of the TWIC holder against the biometric information on the TWIC. TSA conducted a pilot program ending on May 31, 2011, testing the use of TWICs with biometric card readers to help

---

<sup>5</sup> AIT, commonly referred to as body scanners, produces images of the body to screen passengers for metallic and nonmetallic threats including weapons, explosives, and other objects concealed under layers of clothing.

<sup>6</sup> Biometrics refers to technologies that measure and analyze human body characteristics—such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements—for authentication purposes.

<sup>7</sup> See Pub. L. No. 107-295, § 101, 116 Stat. 2064, 2073-74 (2002) (codified as amended at 46 U.S.C. § 70105).

<sup>8</sup> The credential rule established that all maritime workers requiring unescorted access to secure areas of MTSA-regulated facilities and vessels were expected to hold TWICs by September 25, 2008. See 72 Fed. Reg. 3,492 (Jan. 25, 2007). The final compliance date was subsequently extended to April 15, 2009. See 73 Fed. Reg. 25,562 (May 7, 2008).

---

inform the development of a second TWIC regulation, among other purposes.

---

**Additional DHS and  
TSA Actions Needed  
to Validate TSA's  
Behavior-Based  
Screening Program,  
Establish  
Performance  
Measures, and Assess  
Costs and Benefits**

TSA developed the SPOT program in an effort to respond to potential threats to aviation security by identifying individuals who may pose a threat to aviation security, including terrorists planning or executing an attack who were not likely to be identified by TSA's other screening security measures. This program was designed to focus on identifying behaviors and appearances that deviate from an established baseline and that may be indicative of stress, fear, or deception. As we reported in September 2011, TSA had deployed about 3,000 BDOs to about 160 of the approximately 446 TSA-regulated airports in the United States at which passengers and their property are subject to TSA-mandated screening procedures.<sup>9</sup> The following describes progress achieved and challenges faced by TSA in validating the science underlying the SPOT program, developing performance measures, and conducting cost-benefit analysis of SPOT.

**Validation efforts.** TSA has taken actions to validate the science underlying its behavior detection program, but more work remains. In May 2010 we reported that TSA deployed SPOT nationwide before first determining whether there was a scientifically valid basis for using behavior and appearance indicators as a means for reliably identifying passengers who may pose a risk to the U.S. aviation system.<sup>10</sup> We recommended that DHS convene an independent panel of experts to review DHS's efforts to validate the program and determine whether the validation methodology used was sufficiently comprehensive. DHS concurred with our recommendation, and its Science and Technology Directorate completed a validation study in April 2011 to determine the extent to which SPOT was more effective than random screening at identifying security threats and how the program's behaviors correlate to

---

<sup>9</sup> See GAO, *Aviation Security: TSA Has Made Progress, but Additional Efforts Are Needed to Improve Security*, GAO-11-938T (Washington, D.C.: Sept. 16, 2011). In our September 2011 testimony, we cited 463 TSA-regulated airports. TSA has subsequently reduced that number to 446.

<sup>10</sup> See GAO, *Aviation Security: Efforts to Validate TSA's Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges*, GAO-10-763 (Washington, D.C.: May 20, 2010).

---

identifying high-risk travelers.<sup>11</sup> The study found that SPOT was more effective than random screening to varying degrees. However, as noted in the study, the assessment was an initial validation step and was not designed to fully validate whether behavior detection can be used to reliably identify individuals in an airport environment who pose a security risk. In addition, DHS outlined several limitations to the study. For example, the study noted that BDOs were aware that individuals they were screening were referred to them as the result of BDO-identified SPOT indicators or random selection. DHS stated that this had the potential to introduce bias into the assessment, and that additional work would be needed to comprehensively validate the program.

DHS's study made recommendations related to the need for further validation efforts, comparing SPOT with other screening programs, and broader program evaluation issues, some of which echoed recommendations we made in May 2010. DHS's recommendations are intended to help the program conduct a more comprehensive validation of whether the science can be used for counterterrorism purposes in the aviation environment. Given the broad scope of the additional work and needed resources identified by DHS for addressing the recommendations, it could take several years to complete. Officials further stated that it is undertaking actions to address some of these recommendations, such as conducting additional analysis of the program's behaviors and associated SPOT scoring system in coordination with DHS's Science and Technology Directorate.<sup>12</sup> According to TSA, a refined list of the behaviors and appearances used in the SPOT program to identify high-risk passengers will be completed by mid-2012. TSA is taking actions to refine the program, but questions related to the program's validity will remain until TSA demonstrates that using behavior detection techniques can help secure the aviation system against terrorist threats.

---

<sup>11</sup> See DHS, *SPOT Referral Report Validation Study Final Report Volume I: Technical Report* (Washington, D.C.: Apr. 5, 2011). DHS's study defines high-risk passengers as travelers who knowingly and intentionally try to defeat the security process, including those carrying serious prohibited items, such as weapons; illegal items, such as drugs; or fraudulent documents, or those who were ultimately arrested by law enforcement.

<sup>12</sup> TSA developed a scoring system to help determine which passengers exhibited enough SPOT behaviors to be referred to secondary screening or to law enforcement officers for additional screening, or both.

---

According to TSA, as part of its SPOT improvement efforts, TSA is pilot testing revised procedures for BDOs at Boston-Logan and Detroit International Airports to engage passengers entering screening in casual conversation to help determine suspicious behaviors. According to TSA, after a passenger's travel documents are verified, a BDO will briefly engage each passenger in conversation. If more information is needed to help determine suspicious behaviors, the officer will refer the passenger to a second BDO for a more thorough conversation to determine if additional screening is needed. TSA noted that these BDOs have received additional training in interviewing methods. TSA plans to expand this pilot program to additional airports. We will be assessing this pilot as part of a follow-on review of the SPOT program requested by the Chairman of the House Transportation and Infrastructure Committee and plan to report on the results in 2013.

**Performance measures.** Our work on TSA's behavior detection program has underscored the importance of developing sound measures to evaluate the effectiveness of TSA security programs. The Office of Management and Budget (OMB) encourages the use of outcome measures—which track progress toward a strategic goal by documenting the beneficial results of programs—because they are more meaningful than output measures, which tend to be more process oriented or a means to an end.<sup>13</sup> Congress also needs information on whether and in what respects a program is working well or poorly to support its oversight of agencies and their budgets. As we reported in May 2010, TSA had

---

<sup>13</sup> DHS's *National Infrastructure Protection Plan* (Washington, D.C.: June 2006), internal controls standards, and our previous work on program assessment state that performance metrics and associated program evaluations are needed to determine if a program works and to identify adjustments that may improve its results. The NIPP includes a risk management framework that consists of six steps, which closely reflects GAO's risk management framework. (See GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91 (Washington, D.C.: Dec. 15, 2005). Like GAO's framework, the NIPP's risk management framework is a repetitive process that continuously uses the results of each step to inform the activities in both subsequent and previous steps over time. The NIPP risk management framework is designed to produce a systematic and comprehensive understanding of risk and ultimately provide for security investments based on this knowledge of risk.

---

established output-based performance measures<sup>14</sup> for the SPOT program, such as the number of SPOT referrals to law enforcement officers and subsequent arrests; however, it had not fielded outcome-oriented performance measures, such as identifying individuals who may pose a threat to the transportation system, to evaluate the effectiveness of the SPOT program. With such outcome measures, TSA could more fully assess SPOT's contribution to improving aviation security.

As noted in our May 2010 report, SPOT officials told us that it was not known if the SPOT program resulted in the arrest of anyone who is a terrorist or who was planning to engage in terrorist-related activity. According to TSA, in fiscal year 2010, SPOT referred about 50,000 passengers for additional screening and made about 3,600 referrals to law enforcement officers. The referrals to law enforcement officers yielded approximately 300 arrests. Of these 300 arrests, TSA stated that 27 percent were illegal aliens, 17 percent were drug related, 14 percent were related to fraudulent documents, 12 percent were related to outstanding warrants, and 30 percent were related to other offenses. As highlighted in our May 2010 report, we examined the travel of key individuals allegedly involved in six terrorist plots that have been uncovered by law enforcement agencies. We determined that at least 16 of the individuals allegedly involved in these plots moved through 8 different airports where the SPOT program had been implemented. In total, these individuals moved through SPOT airports on at least 23 different occasions.<sup>15</sup>

In May 2010, we recommended that to better measure the effectiveness of the program and evaluate the performance of BDOs, TSA should

---

<sup>14</sup> According to OMB Circular No. A-11, outputs describe the level of activity that will be provided over a period of time, including a description of the characteristics (e.g., timeliness) established as standards for the activity. They also refer to the internal activities of a program (i.e., the products and services delivered). Output measures help determine the extent to which an activity was performed as planned. Outcome-related measures are more robust measures because they provide a more comprehensive assessment of the success of the agency's efforts, as stated in DHS's 2009 NIPP.

<sup>15</sup> For example, according to Department of Justice documents, in December 2007 an individual who later pleaded guilty to providing material support to Somali terrorists boarded a plane at the Minneapolis-Saint Paul International Airport en route to Somalia to join terrorists there. Similarly, in August 2008 an individual who later pleaded guilty to providing material support to al-Qaeda boarded a plane at Newark Liberty International Airport en route to Pakistan to receive terrorist training to support his efforts to attack the New York subway system.

---

establish a plan that includes objectives, milestones, and time frames to develop outcome-oriented performance measures.<sup>16</sup> DHS concurred with our recommendation while noting that it is difficult to establish measures for a deterrence-based program. According to TSA, the agency has recently developed a metrics framework, which includes process measures, output measures, and outcome measures, that will allow SPOT programs at each airport to measure their improvement year by year. After the framework is validated by DHS's Science and Technology Directorate and subject matter experts, TSA expects to roll out this metrics framework as part of TSA's general performance management system in the fourth quarter of fiscal year 2012. We plan to assess this framework as part of our recently initiated review of SPOT.

**Cost-Benefit Analysis.** As we reported in May 2010, TSA did not complete a cost-benefit analysis before deploying the SPOT program. According to the DHS National Infrastructure Protection Plan, security strategies should be informed by, among other things, a risk assessment that includes threat, vulnerability, and consequence assessments; information such as cost-benefit analyses to prioritize investments; and performance measures to assess the extent to which a strategy reduces or mitigates the risk of terrorist attacks.<sup>17</sup> Our prior work has shown that cost-benefit analyses help congressional and agency decision makers assess and prioritize resource investments and consider potentially more cost-effective alternatives, and that without this ability, agencies are at risk of experiencing cost overruns, missed deadlines, and performance shortfalls.<sup>18</sup>

In May 2010, we reported that TSA did not conduct such an analysis of SPOT prior to full-scale nationwide deployment, and we recommended that it do so, including a comparison of the SPOT program with other security screening programs, such as random screening, or already existing security measures. DHS concurred with our recommendation and noted that TSA was developing an initial cost-benefit analysis. However, it was not clear from DHS's comments whether its cost-benefit analysis

---

<sup>16</sup> GAO-10-763.

<sup>17</sup> DHS, *National Infrastructure Protection Plan*. In 2009, DHS issued an updated plan that replaced the one issued in 2006.

<sup>18</sup> See GAO, *Homeland Security: DHS and TSA Acquisition and Development of New Technologies*, GAO-11-957T (Washington, D.C.: Sept. 22, 2011).

---

would include a comparison of the SPOT program with other TSA security screening programs and existing security measures as we recommended. As of March 2012, TSA has not conducted a cost-benefit analysis, which could help the agency establish the value of the program relative to other layers of aviation security. Moreover, a cost-benefit analysis could also be useful in considering future program growth. The program's budget has increased from \$198 million in fiscal year 2009 to a requested \$227 million in fiscal year 2013, a 15 percent increase over 5 years. In March 2012, TSA officials stated that TSA has developed a "risk and cost analysis framework," which has been applied to several different TSA programs, such as its AIT. TSA is refining the framework in order to complete the risk and cost analysis work for SPOT BDOs, which could provide TSA management with additional information on whether its BDO allocation is a prudent investment. We will be assessing this issue as part of our recently initiated review of SPOT.

---

### Full-Body Scanners Not Fully Utilized at Some Airports

As we reported in March 2010, in response to the December 25, 2009, attempted bombing of Northwest flight 253, the Secretary of Homeland Security announced five corrective actions to improve aviation security, including accelerating deployment of AIT to identify materials such as those used in the attempted Christmas Day bombing.<sup>19</sup> According to TSA officials, AIT was to provide enhanced security benefits compared to walk-through metal detectors, such as enhanced detection capabilities for identifying nonmetallic threat objects and liquids.

In January 2012, we issued a classified report on TSA's procurement and deployment of AIT, commonly referred to as full body scanners, at airport checkpoints.<sup>20</sup> As of March 2012, TSA has deployed about 640 AIT units to 165 TSA-regulated airports. Among other things, we reported instances where AIT units were not being used, which raised questions about the

<sup>19</sup> See GAO-10-484T. The other four actions include modifying the criteria used to create terrorist watch lists, establishing a partnership between DHS and the Department of Energy and its national laboratories to develop new technologies to deter threats to aviation, strengthen the presence of Federal Air Marshals aboard U.S.-bound flights, and working with international partners to strengthen international security measures and standards for aviation security.

<sup>20</sup> Details from this section were removed because TSA deemed them Sensitive Security Information, which must be protected from public disclosure pursuant to 49 C.F.R. part 1520.

---

cost-effectiveness of this acquisition. We analyzed TSA's utilization data collected from March 2010 through February 2011 on all deployed AIT units and found that some deployed units were not used regularly, decreasing their potential security benefit. During this time period, some of the deployed AIT units were used on less than 5 percent of the days they were available since their deployment.<sup>21</sup> Additionally, some units were used on less than 30 percent of the days available since their installation.<sup>22</sup> Moreover, we reported that at some of the 12 airports we visited, AIT units were deployed but were not regularly used. For example, at one airport we observed that TSA had deployed 3 AIT units in an airport terminal that typically handles one flight a day of approximately 230 passengers. TSA officials reported that 2 of the AIT units were seldom used because of the lack of passengers and stated that they believed the AIT units were deployed based on space constraints in areas where they could be placed. According to the Federal Acquisition Regulation, acquisition begins at the point when agency needs are established and includes, among other things, the description of requirements to satisfy agency needs.<sup>23</sup> The limited use of some of these machines may indicate that there was not a clear need for them at the time they were acquired at the locations in which they were deployed. Each AIT unit costs approximately \$250,000 to acquire and install. Additionally, each AIT unit is budgeted for five full-time equivalent (FTE) personnel, each of which costs approximately \$63,000 per year.<sup>24</sup> Using these figures, we estimate that the first year total cost—including acquisition, installation, and equipment operator salary—was several million dollars.<sup>25</sup> In January 2012, we made a recommendation to TSA to study current AIT utilization and address the extent to which currently

---

<sup>21</sup> The specific number of AIT units used on less than 5 percent of the days available since their deployment was deleted because it is considered Sensitive Security Information.

<sup>22</sup> The specific number of AIT units used on less than 30 percent of the days available since their installation was deleted because it is considered Sensitive Security Information.

<sup>23</sup> See 48 C.F.R. § 2.101.

<sup>24</sup> We estimated that the 486 AIT units deployed at the time would cost approximately \$153 million in labor to operate per year. This was based on 5 FTEs per unit and the average TSO salary and benefit cost of \$63,000.

<sup>25</sup> We did not include the specific cost information in the public version of the report as it would identify the number of AIT units in question, which is considered Sensitive Security Information.

---

deployed AIT units are used. TSA concurred with our recommendation and plans to take efforts to address it.

---

### Additional Actions Needed to Strengthen Internal Controls and Address TWIC Effectiveness

The TWIC program is intended to improve maritime security by using a federally sponsored credential to enhance access controls to secure areas at MTSA-regulated facilities and vessels. As of March 20, 2012, the TWIC program has enrolled over 2.1 million maritime workers and issued nearly 2 million credentials. The TWIC is to be used by individuals requesting unescorted access to MTSA-regulated facilities and vessels and currently is to be visually inspected by facility and vessel operators. The following describes progress made and challenges faced by DHS related to the TWIC program's system of internal controls and DHS's efforts in assessing the effectiveness of TWIC.

**Internal Controls.** DHS has established a system of TWIC-related processes and controls to assist in implementation of the program. In May 2011, we reported that internal control weaknesses governing the enrollment, background checking, and use of TWIC potentially limit the program's ability to meet the program's stated mission needs or provide reasonable assurance that access to secure areas of MTSA-regulated facilities is restricted to qualified individuals.<sup>26</sup> Key program weaknesses included an inability to provide reasonable assurance that only qualified individuals can acquire TWICs or that once issued a TWIC, TWIC holders have continued to meet eligibility requirements.

As we reported in May 2011, to meet the stated program purpose, TSA's focus in designing the TWIC program was on facilitating the issuance of TWICs to maritime workers. However, TSA did not assess the internal controls in place to determine whether they provided reasonable assurance that the program could meet defined mission needs for limiting access to only qualified individuals.<sup>27</sup> For example, controls that the TWIC

---

<sup>26</sup> GAO, *Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives*, GAO-11-657 (Washington, D.C.: May 10, 2011).

<sup>27</sup> In accordance with GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999), the design of the internal controls is to be informed by identified risks the program faces from both internal and external sources, the possible effect of those risks, control activities required to mitigate those risks, and the cost and benefits of mitigating those risks.

---

program had in place to identify the use of potentially counterfeit identity documents were not used to routinely inform background checking processes. Additionally, controls were not in place to determine whether an applicant has a need for a TWIC. Further, TWIC program controls were not designed to provide reasonable assurance that TWIC holders maintained their eligibility once issued TWICs. For example, controls were not designed to determine whether TWIC holders have committed disqualifying crimes at the federal or state levels after being granted a TWIC.

We further reported that internal control weaknesses in TWIC enrollment, background checking, and use could have contributed to the breach of selected MTSA-regulated facilities during covert tests conducted by our investigators. During these tests at several selected ports, our investigators were successful in accessing port facilities using counterfeit TWICs, authentic TWICs acquired through fraudulent means, and false business cases (i.e., reasons for requesting access). Our investigators did not gain unescorted access to a port where a secondary port-specific identification was required in addition to the TWIC. TSA and Coast Guard officials stated that the TWIC alone is not sufficient and that the cardholder is also required to present a business case. However, our covert tests demonstrated that having an authentic TWIC and a legitimate business case were not always required in practice.

In our May 2011 report, we recommended that the Secretary of Homeland Security perform an internal control assessment of the TWIC program by (1) analyzing existing controls, (2) identifying related weaknesses and risks, and (3) determining cost-effective actions needed to correct or compensate for those weaknesses so that reasonable assurance of meeting TWIC program objectives can be achieved. DHS officials concurred with our recommendations. As of March 2012, DHS reported that it had initiated a review of current internal controls, established a working group with executive oversight to develop and implement solutions to these recommendations, and completed a number of short-term actions to partially address some of the weaknesses. We plan to assess these actions as part of our review of the TWIC pilot and will issue a report on our assessment later this year.

**TWIC's Effectiveness.** As we reported in May 2011, DHS asserted that the absence of the TWIC program would leave America's critical maritime

---

port facilities vulnerable to terrorist activities.<sup>28</sup> However, to date, DHS has not assessed the effectiveness of TWIC at enhancing security or reducing risk for M TSA-regulated facilities and vessels. Further, DHS has not demonstrated that TWIC, as currently implemented and planned with card readers, is more effective than prior approaches used to limit access to ports and facilities, such as using facility-specific identity credentials with business cases (i.e., reasons for requesting access).

According to TSA and Coast Guard officials, because the program was mandated by Congress as part of M TSA, DHS did not conduct a risk assessment to identify and mitigate program risks prior to implementation. However, internal control weaknesses raise questions about the effectiveness of the TWIC program. Moreover, as we have previously reported, Congress also needs information on whether and in what respects a program is working well or poorly to support its oversight of agencies and their budgets, and agencies' stakeholders need performance information to accurately judge program effectiveness. Therefore, we recommended in our May 2011 report that the Secretary of Homeland Security conduct an effectiveness assessment that includes addressing internal control weaknesses and, at a minimum, evaluate whether use of TWIC in its present form and planned use with readers would enhance the posture of security beyond efforts already in place given costs and program risks. We further recommended that the internal control and effectiveness assessments be used as the basis for evaluating the costs, benefits, and security risks of the TWIC program prior to requiring the use of TWICs with card readers. DHS concurred with our recommendation. As of March 2012, DHS reports that it is further evaluating the TWIC program using its risk assessment model. This step could help inform DHS of the TWIC program's effectiveness.

---

Chairmen Issa and Mica, Ranking Members Cummings and Rahall, and Members of the Committees, this concludes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

---

<sup>28</sup> See DHS, *Transportation Worker Identification Credentialing (TWIC)*, DHS Exhibit 300 Public Release BY10/TSA (Washington, D.C.: Apr. 17, 2009), and *Transportation Worker Identification Credentialing (TWIC)*, DHS Exhibit 300 Public Release BY09/TSA (Washington, D.C.: July 27, 2007).

Chairman ISSA. Admiral?

**STATEMENT OF REAR ADMIRAL PAUL F. ZUKUNFT**

Admiral ZUKUNFT. Good afternoon, Chairman Issa and distinguished members of the committees. I am honored to appear before you today to speak about the Coast Guard's role in enforcing compliance with the Transportation Worker Identification Credential, or TWIC, program within the maritime transportation system.

The TWIC program, as envisioned under the Maritime Transportation Security Act, or MTSA, of 2002 and strengthened by the SAFE Port Act of 2006, requires that all credentialed merchant mariners and transportation workers seeking unescorted access to secure areas of MTSA-regulated facilities and vessels undergo a security check and receive a TWIC. The TWIC is currently required for unescorted access to approximately 2,700 regulatory facilities, 12,000 regulated vessels, and 50 regulated Outer Continental Shelf facilities.

While the Transportation Security Administration has primary responsibility for the issuance of TWICs, the Coast Guard has primary responsibility for ensuring compliance with the TWIC regulations. All of the approximately 2,700 maritime facilities impacted by the TWIC regulations are and have been in compliance since the April 15th, 2009, implementation date. The Coast Guard continues to conduct both unannounced and announced inspections to ensure compliance. Additionally, the Coast Guard has verified more than 213,000 TWICs through a combination of visual and electronic means.

In accordance with the SAFE Port Act, a pilot program was conducted by TSA to evaluate the feasibility and technical and operational impacts of implementing a TWIC reader system. Electronic readers add another layer of security associated with the TWIC by providing biometric confirmation of the TWIC holder's identity. TSA's report on the pilot program was delivered to Congress on February 27th, and the Coast Guard is now incorporating the results of the pilot in our rulemaking for electronic readers in the maritime environment. This rulemaking will apply requirements in a risk-based fashion to leverage security benefits and capabilities.

Additionally, Section 809 of the Coast Guard Authorization Act of 2010 amended the original TWIC requirements to include only those mariners allowed unescorted access to a secure area designated in a vessel security plan. As elements of the Coast Guard merchant mariner credential issuance process relies upon data received through TWIC enrollment, the provision was neither self-executing or easily implemented. Noting such, the Coast Guard issued a policy letter in December 2011 to remove the requirement to hold a TWIC for mariners currently inactive or those serving on vessels that do not require a vessel security plan. The Coast Guard continues to work toward codification of this change through a rulemaking process.

A GAO report on TWIC in May 2011 identified a weakness in verification of TWICs in the field. In response, we issued policy to our field units directing thorough verification of TWICs at checkpoints, highlighting that a quick flash of the TWIC was not acceptable. The electronic readers deployed at our units ensure each per-

son attempting to enter a facility is carrying a TWIC. And, to date, we have implemented over 275 readers to our field units.

We continue to work with our DHS partners and particularly with TSA, as well as State and local agencies, to continue to improve the TWIC program for seafarers and other maritime transportation workers by balancing a steadfast commitment to security while facilitating commerce.

Thank you for the opportunity to appear before you today. I will be pleased to answer your questions.

Chairman ISSA. Thank you.

Chairman ISSA. And as earlier announced, we will now recognize the gentleman from Maryland for his opening statement.

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

Today, the Oversight Committee and the Transportation and Infrastructure Committee convene to examine measures TSA utilizes to secure our Nation's transportation networks.

In the realm of aviation security, the TSA must achieve a delicate balance. TSA must be effective in meeting the evolving threats posed by terrorists. We also expect it to be responsive to the needs of the public and the demands of commerce.

Since the terrible events of September 11th, 2001, several attacks have been attempted against commercial planes, including the attempted bombing on Christmas Day 2009 of Northwest Airlines Flight 253 and the attempted bombing in 2010 of a cargo jet using a bomb disguised as an inkjet cartridge. These incidents demonstrate the constantly evolving threats TSA must counter.

TSA's 43,000 transportation security officers must screen more than 2 million passengers every day in our Nation's 450 airports. Although the vast majority of passengers pose no risk, these officers must find the equivalent of a needle in a haystack.

In response to the Christmas Day bombing attempt, TSA increased its deployment of advanced imaging technology systems to screen passengers for both metallic and non-metallic threats. More recently, TSA has developed the PreCheck program to expedite screening for low-risk travellers, such as members of the military.

I welcome TSA's efforts to develop a more intelligent, risk-based approach to transportation security. Recognizing the enormity of the challenge TSA faces, as the agency develops new screening techniques we must ensure that it strikes the appropriate balance between moving too quickly to deploy untested or unreliable technologies or techniques and moving too slowly to address new threats.

Today's hearing will also review the Transportation Worker Identification Credential. When I served as chairman of the Subcommittee on Coast Guard and Maritime Transportation, I convened hearings in 2007 and 2008 to review the rollout of TWIC. And I thank the Coast Guard for joining us today.

Unlike many screening techniques TSA uses in the aviation realm, Congress mandated what became the TWIC program and required that this program be funded by fees collected from enrollees. There are now more than 2.1 million enrollees, and, by our estimate, these enrollees have paid approximately \$280 million to implement this program.

To close the security perimeter that TWIC is intended to create, we must finally implement the use of readers so that these cards are no longer just expensive flash passes. TSA must also ensure that TWICs are not issued to ineligible applicants.

However, we must also view TWIC in the broader maritime security context. TWIC is meant to control land-side access to secure areas of U.S. ports and secure areas of U.S. vessels. There are many risks that approach our ports, particularly from the water side, that TWIC was never intended to address. None of the individuals on the estimated 17 million small boats operating in our waters are required to carry TWICs, and none of the foreign mariners on the more than 9,000 foreign-flagged vessels calling on U.S. ports carry TWICs.

Our first and most critical line of maritime defense, our thin blue line at sea, is the Coast Guard, which must defend our coasts, rescue thousands at sea, respond to marine casualties and oil spills, intercept drugs and migrants, and enforce security requirements at 2,500 facilities and on nearly 13,000 vessels regulated by the Maritime Transportation Security Act.

This service of 42,000 active-duty officers and members do all of this on a budget of less than \$10 billion per year, less than 2 percent of the DOD's base budget. And they now face additional cuts and the loss of up to 1,000 active-duty slots in next year's budget.

The Coast Guard does all that we ask of them to do. However, we cannot continue to stretch the service and assume that it will never break or that gaps will not open in our maritime security.

With that, Mr. Chairman, I yield back, and I want to thank you for your courtesy.

Chairman ISSA. I thank the gentleman.

Chairman ISSA. We have also been joined by the chairman of the full Transportation Committee, and I now recognize him.

Mr. MICA. First of all, thank you so much, Chairman Issa, and to your committee, Government Reform and Oversight. I am honored to co-chair this hearing with you. I am sorry there was a little bit of a delay getting back here today, but pleased to be with you. And I thank you for your leadership on this.

This is a very important agency that we have joint responsibility over. Our committee has some limited oversight responsibility. Under Transportation, as you may recall, historically, TSA was created. I happened to chair the Subcommittee on Aviation in 2001 after the horrific terrorist attacks.

Since that time, TSA has grown from 16,500 screeners and a small cadre of different transportation security activities which we joined together. It was a much smaller beginning, and, unfortunately, TSA has mushroomed to 65,000 employees, of which there are 14,000 administrative personnel—4,000 in Washington and 10,000 out in the field.

We never intended it to mushroom to this size. And, as you know, I have been critical particularly of the administrative cost. Even with the administrative cost, we might be able to endure that kind of expenditure, which has now grown to \$8 billion, if it meant we were secure. But instead, as this committee report today reviews, we have a number of programs that are so far behind.

One that I would like to talk about is the TWIC program, Transportation Worker Identification Card. We have spent hundreds of millions of dollars, and it is still in limbo. Some of the equipment that has been purchased does not do the job. I know we can't talk about all of it here in this open setting. But the deployment and acquisition of expensive equipment that is supposed to protect us, which wasn't properly tested, vetted, and the deployment could have probably have been done better by a high school class project.

TSA has had five Administrators in 9 years. We had a period under the Obama administration in which we had no Administrator for almost a year. It is difficult enough with an agency like TSA or any other Federal agency to operate with an Administrator in Washington, let alone not having an Administrator for that period of time.

I have other concerns, having monitored this as closely as anyone in Congress. We are still at risk; the Nation is still at risk. Unfortunately, even the layered system—and TSA will talk to you about a layered system. Almost every layer is just flawed. The behavior detection, which I worked with previous Administrators to put in—when we had equipment that didn't work, TSA again bought equipment that didn't work. Just following that equipment, the puffers—and I have had my investigative staff follow that—they sat and we were paying rent on them on a vacant—I am sorry, in a warehouse that then they spent \$600, I think, per piece of equipment. They told us that DOD had them destroyed, but only after we prompted the action.

Sent investigators down to look at another—jointly, we sent them down to look at another warehouse we had gotten information that was full of equipment, some of it purchased, some of it should have been deployed, some of it sitting there at great taxpayer expense for a long time paying rent on it.

And then the nerve to cause us to delay—and I might even ask if we can't get the information to subpoena it—when we were informing TSA that we were sending our investigative staff there, to delay our staff and investigation by a week so trucks could come up and haul this stuff away, even some as our investigators were appearing on the scene.

It is just a very expensive and disappointing operation. I have had faith in Administrator Pistole. He promised reform. He has told the committee he would reform the agency. And I don't see that happening, unfortunately.

But that is just the highlights, Mr. Chairman. It is just important that we get to the bottom of this. There is a lot of hard-earned taxpayer money going for, unfortunately, theater security, not real security. And we have to stop paying that price before we pay a huge price with another successful attack by terrorists.

I yield back the balance of my time.

Chairman ISSA. I thank the gentleman.

I will now recognize myself for 5 minutes.

I have the advantage of knowing your bios. You may not know mine, but I spent nearly 3 decades in security. And the one thing I know about security is, there are two types. There is the type that convince people that your target is harder than somebody else's. In other words, I can't protect all cars, but I can make the

crook choose to steal the car next to the one protected by Viper. That is what I would say you have as a system here today.

You, in fact, have a series of hardenings. They work sometimes. And I am speaking particularly about in the aviation. These programs certainly seem to be good programs. And in every case, as the wind blows through the screen, those spots clearly will at times stop targets. But targets, particularly terrorist targets, are in fact exactly like you would expect: They are mobile, they are responsive.

If we do not have a layered security system that has a sufficient force to at least be like the hull of a ship, Admiral, one in which we know there will be a few leaks that you have to pump out but for the most part it is watertight—our security system today is clearly not watertight.

The accidental catching of the bad guys belabors two points: one, the many people who in fact find themselves, like most of us on the dais, going through security and sometimes they have us pull something out, sometimes they don't; sometimes they do a secondary, sometimes they don't.

I am going to give you just a couple. We opened up this hearing to Facebook. I am just giving you anecdotal ones, but I will supply all of them. I will place them in the record, and I will also supply all of them to you so you can respond to the individuals in their entirety.

But, for example, Joe Carica. He is a U.S. Marine. He was flying in his Dress Blues "D" uniform. He was forced to remove his trousers in full view of passengers because his shirt-stays beneath them were scaring a TSA employee. It didn't matter that he explained what it was, and it didn't matter that they were something that he undoubtedly had seen many times before if he were a veteran. Of course, you and I all know that the turnover at TSA is high and the training is seemingly perpetual.

The next one is from Reagan Shea, who says, "I am a disabled person and have been targeted for groping. My wife travels with a portable oxygen concentrator, and her use of the machine means she get pawed by hand every time we travel."

Julia Rachiele: "The TSA has taken away my freedom to travel because I wear a medical device and cannot go through the amount of radiation I would be subjected to. As a result, I get an enhanced pat-down procedure every time."

Lastly—and there are plenty more; there are over 350—"I am Wendy. I have worn an artificial leg since I was 4. I am now 61. I used to travel a lot for my work but gave up traveling after being assaulted by TSA constantly, even to the point of having my breasts checked instead of my leg prosthesis."

First question I have for the panel, and particularly for the aviation side: There are 65,000 to 67,000 TSA workers, men and women who are trying to do a good job. A quarter of them are employed in administration.

First question for you is, do you think that is a fair ratio of administration? Or do you think you are, in fact, a bloated, bureaucratic organization that has a lot of people working on a lot of systems that ultimately, after procurement, don't work?

Mr. McLaughlin?

Mr. McLAUGHLIN. Sir, I will respond to that. First of all, thank you for recognizing the very hardworking men and women of TSA. Our folks in the field are working hard every day to keep all of us safe as we travel.

I will have to take for the record the ratio for administrative to frontline personnel. I think it might be different from that, but I will get back to you.

Chairman ISSA. Well, I will give you one—I travel, obviously, to a number of places—Houston, Sacramento—but San Diego and Dulles are my two majors. I can tell you that I periodically count, and for 4 active checkpoints in San Diego there will be as many as 35 people in blue standing there.

So even if your administrative count were not one in four, wouldn't you agree, based on your own observations, that the amount of people directly at a checkpoint versus the total number would seem to be extremely high? In other words, you haven't created any efficiency in the 10 years of your existence.

Mr. McLAUGHLIN. Well, certainly, I don't agree with that. TSA is working hard to provide the most effective—

Chairman ISSA. Well, let's go through the numbers, though, quickly. Because I am really on overtime, and I will make it up to the ranking member.

There are four times as many TSA employees as there was 7 or 8 years ago, correct?

Mr. McLAUGHLIN. Again, I don't believe—

Chairman ISSA. In 2002, 16,000 in your initial authorization, so you had less than that. By 2005, you were still below 35,000. You are now over 65,000. In the last, let's say, 5 years, when you have more than doubled in numbers, have the American people seen shorter lines? Yes or no?

Mr. McLAUGHLIN. I do believe that the American people have seen shorter lines in the last 4 or 5 years.

Chairman ISSA. Yeah. Well, with that, I would like you to check your figures. The fact is, they haven't seen shorter lines. I fly to enough airports to tell you that, in fact, you are not giving shorter lines. You are taking longer for each one and using more people.

With that, I would recognize the ranking member for his questions.

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

TSA recently completed the reader pilot test required by the SAFE Port Act. And as I mentioned in my opening statement, I believe that to maximize the security TWIC can provide, we must move to implement the use of the readers.

Assistant Secretary Sadler, TSA was responsible for the recent reader pilot test. And, Admiral Zukunft, the Coast Guard is responsible for promulgating the final reader rule. Let me ask both of you this: Will it be technically feasible for facilities to install readers that can quickly and reliably read TWIC cards without impeding the flow of workers into ports and to the secure areas of vessels? And by what date do you think the installation of the readers can realistically be achieved?

And I think we have been—it seems like we ought to be able to get this done, gentlemen, some kind of way. We have been messing around with this for a while.

Oh, come on, some of you, one of you. Admiral?

Admiral ZUKUNFT. Ranking Member, I would be pleased to answer that.

As you know, we have embarked upon the rulemaking process. Getting to a final rule, before we do that we really need to adjudicate the comments. So that would be very informative to answer that very question, with the objective of not impeding commerce.

There are over 32 recognized commercial-off-the-shelf TWIC readers. We expect one of the concerns will be, you know, whether you use a mobile system or whether it is a fixed system that would be at a container terminal. But we would envision approximately a 2-year period of time from the time a final rule was on the street to full implementation across industry.

Mr. CUMMINGS. Mr. Sadler, do you have a response?

Mr. SADLER. Yes. I think, sir, during the pilot we did show that when the readers were installed properly, the people who worked in the facilities were trained properly, and the workers were assimilated to the cards and the use of the cards with those readers, that they did work properly. They did not impede the flow of commerce in those particular ports.

But it does depend on the installation, it does depend on the training, and it does depend on whether the facility has picked the right reader for its business need.

Mr. CUMMINGS. Okay.

Admiral Zukunft, the GAO reported that its employees were successful in accessing ports using counterfeit TWICs—authentic TWICs acquired through fraudulent means in false business cases.

Let me ask you this. I want you to clarify that individual ports still have the authority, and indeed the responsibility, to deny admission even to those who have valid and authentic TWICs if they have no business on the port property. Is that correct?

Admiral ZUKUNFT. That is correct.

Mr. CUMMINGS. And, that said, what steps has the Coast Guard taken to address the GAO's findings? And, additionally, do you think the use of readers will help close these security gaps?

Admiral ZUKUNFT. Ranking Member, I do. We have issued policy guidance to our field units. To date, they have been out in the field screening, doing spot checks. We have done over 200,000 of these spot checks. In a 2-day period alone last week, we ran over 450 spot checks. And out of those 450, we did find 58 members who had no rightful business being at those particular facilities.

We engage extensively with our stakeholders through our security committees and certainly the facility owners. They are interested, first of all, in those who may have criminal intent, which is one of the slices of information that TWIC provides. And on a steady basis, that pool of 2 million TWIC card holders are being screened against the terrorist screening database. So there is realtime information but also a benefit to the facility owners as well.

Mr. CUMMINGS. Yeah, TWIC is the only part of our maritime security regime that—and that is very significant. The Coast Guard is and will remain the most important element of that regime, but the strains of budget cuts on the service are obvious. For example, in 2010, 10 of the 12 cutters deployed to respond to the earthquake

in Haiti suffered significant problems, and 2 had to be taken out of service and sent in for major repairs. Is that right?

Admiral ZUKUNFT. I was intimately involved with that response, Ranking Member, and that is true.

Mr. CUMMINGS. And in February of this year, the GAO issued a new report finding that, in part due to a lack of funding, the Coast Guard does not have any fully operating interagency operating centers, though these were required by the SAFE Port Act to be established by October 2009.

Similar to the GAO, the DHS inspector general and others have noted the Coast Guard's inability to meet safety and security mission requirements in the Arctic as the ice cover opens to allow more shipping operations in those latitudes. Nonetheless, the President's budget proposes extensive cuts both to the Coast Guard's end strength and its capital account. No funding was requested for the acquisition of the National Security Cutter 7 or 8. And this budget will conclude the acquisition of the Fast Response Cutter at a number substantially below the approved program of record.

Finally, this is my last question. While I know that the Coast Guard strives to meet every mission requirement, can you comment on the challenges the service is facing in balancing its competing mission needs, particularly in the maritime security arena, in light of the significant budget constraints?

I have always complained about the Coast Guard not having enough money. I am just trying to figure out how you are going to do all the things you have to do, particularly since 9/11, with regard to the budget cuts.

Admiral ZUKUNFT. I would be pleased to, Ranking Member Cummings.

I was involved in the Deepwater Horizon oil spill. I was the Federal on-scene coordinator for over 7 months. And the President directed that we triple our response effort.

The Coast Guard has no force in garrison; we are constantly doing frontline operations. And so we had the good fortune, if you want to call it that, where we didn't have another contingency occurring at the same time as Deepwater Horizon, so I was able to redeploy buoy tenders from Cordova, Alaska, to Honolulu and marshal all of those resources into the Gulf of Mexico. We were able to do the same during the earthquake in Haiti, even though some of those ships did have maintenance challenges, and we did the same during Hurricane Katrina.

So the challenge we face in the maritime security domain is, what if we have multiple threats? What if we have a hurricane and then we have a threat to national security taking place concurrently? And that is where we really run into resource challenges, because we have to reallocate resources from one mission to another. And we are at risk because we don't have the resources to do both.

Mr. CUMMINGS. Thank you very much.

Chairman ISSA. I thank the gentleman.

We now recognize the chairman of the full committee, Mr. Mica, for 5 minutes.

Mr. MICA. Well, first of all, my friends at TSA and other witnesses, since my last hearing, which was with the Appropriations

subcommittee—I am not a member of that subcommittee but was allowed to ask questions, as we have extended to others who are not on our committee. And——

Chairman ISSA. We recommend that system to all committees.

Mr. MICA. Well, yes. And the funny thing about that is, Mr. Chairman—and I won't allow this to take away from my time, but I have to put this caveat in. TSA found out that I would be a witness, so they sent Mr. Pistole an email. The email said, "Mr. Mica is going to be there, so when he asks a question, Mr. Pistole, take a long time answering it so you eat up his time." The problem is that they—again, sometimes you think it is the gang that can't shoot straight, but they shot the email to CQ. I think that was the publication.

So, again, reserving my time, if you would answer fairly briefly and not use the directive of that memo. One of my concerns, of course, is the Transportation Worker Identification Card. We have spent over a half a billion dollars, is that correct? Yes or no? Mr. McLaughlin? Mr. Sadler?

Mr. SADLER. I will take that one, sir. To date——

Mr. MICA. I have \$511 million spent.

Mr. SADLER. To date, on the program itself, we have expended approximately \$374 million.

Mr. MICA. But I have \$511 million.

Mr. SADLER. You may be including grants in that. I would have to go back and check that number.

Mr. MICA. Well, we wouldn't want to leave any—I mean, I consider that as an expenditure, money spent. All right, well, we will say in the neighborhood of a half a billion.

And the card is supposed to allow us to identify who goes into our ports. We passed the law setting that requirement up back after 2001, right, Mr. Sadler? Who wants to answer?

Mr. SADLER. I believe that was required by the MTSA of 2002.

Mr. MICA. 2002, after 2001. Thank you.

They have produced—1.9 million of the cards are active, printed 2.1 million of them. We still do not have all of the components that were required under the law, including iris and thumbprint, as far as biometric capability, do we, Mr. Sadler?

Mr. SADLER. We have the capability to include an iris on the chip of the card.

Mr. MICA. But you do not have a standard for iris, right?

Mr. SADLER. That is correct. NIST has just put out a proposed change to the standard to include iris.

Mr. MICA. Again, I just have to go back because this is not going to be Groundhog Day, but I had a hearing April 14th, almost a year ago, and the director of the NIST Information Technology Lab testified. And I have the questions here. "When will you finish the iris capability?" "Draft publication will be"—this is last year—"hopefully before next week." "And when will you finish the final standard?" "By the end of the year." That was last year.

Now, I was told at the beginning of the year it might be, what? This summer? Is that what you have heard?

Mr. SADLER. No, sir, I haven't gotten a time for when the——

Mr. MICA. So don't have a time. They told us this summer. So we are now going into our ninth year.

Now, it is great that we produced these TWIC cards at great public expense, a half a billion, but then I read that you are still in a pilot reader program. So, basically, we have 1 million of these cards and we don't have readers; is that correct?

Mr. SADLER. Well, just to go—

Mr. MICA. Do the ports have readers?

Mr. SADLER. —just to go back a second—

Mr. MICA. Do the ports have readers?

Mr. SADLER. —there is a fingerprint template on the chip of the card.

Mr. MICA. Do the ports have readers?

Mr. SADLER. Certain ports do have readers. And we have 35 readers that are—

Mr. MICA. Do we have—

Mr. SADLER. —on our approved products list that the ports can use.

Mr. MICA. How many of the ports would have readers, and how many of these cards are able to be read?

Mr. SADLER. Well, we know—

Mr. MICA. As a percentage.

Mr. SADLER.—we know that the pilot ports have readers. I don't know the number of ports outside of the pilot ports that have readers. I do know the Coast Guard has—

Mr. MICA. Staff, can we insert in the record at this time the very small number of ports that in fact have readers? And we don't—  
Chairman ISSA. Without objection, so ordered.

Mr. MICA. Thank you.

Behavior detection, let me go into this. And I am just going to take 1 more minute, because I had to—

Chairman ISSA. Without objection, so ordered.

Mr. MICA. Behavior detection program, we have spent a billion dollars on it. Can someone—can someone say that that is correct?

Mr. MCLAUGHLIN. Sir, I believe that number is slightly below that, but we will get back to you for the record.

Mr. MICA. Okay. All right.

And I also—I asked—when I knew that the puffers didn't work, that they had bought and told me that they would work, and actually went up and had them tested, went through, every time it didn't detect some trace elements that were put on me, I was told it was just a technical problem. And we just destroyed those; is that correct? We paid \$600 a piece to destroy the puffers; is that correct?

Mr. MCLAUGHLIN. I believe that is correct.

Mr. MICA. I don't even want to know how long they sat in the warehouse, and then they had DOD destroy them. But getting something else in place because the technology didn't work, and you all have seen the classified reports on the performance of the advanced imaging technology equipment, have you not?

Mr. MCLAUGHLIN. Yes.

Mr. MICA. So we know by that performance and the lack of performance of what we have seen with the puffers, that behavior detection is very important and others use it successfully. The problem is GAO reviewed the performance and said that 24 times, 17 known terrorists went through airports, passed TSA, and they have

yet to detect one terrorist. And that was actually a question that was submitted by one of the Floridians we had open question online that we allowed people. Can you name any terrorists that you have actually stopped in the program?

Mr. McLAUGHLIN. We are not aware of any terrorists transiting a checkpoint where BDOs were actively working. While we accept GAO's comments that there were 24 instances in SPOT airports, we do not know that BDOs were working at the time that those individuals came through, number one. And number two, we know, in hindsight, they were not operational, so they were not exhibiting signs of stress, fear, or deception.

Mr. MICA. Thank you.

Mr. LORD. May I comment on that?

Chairman ISSA. Yes. The gentleman's time has expired.

Mr. LORD. I am the GAO representative. I think our point in the report was to study the travel patterns that people associate with terrorists to see if they were exhibiting any SPOT behaviors. At this time, I don't believe it is known whether they were exhibiting behaviors or not. And we made that recommendation in the spirit of improving the program to develop better performance measures. We suggested reviewing the videotapes; we thought that would be a rich source of information to help refine the program.

Mr. MICA. At this point, Mr. Chairman, I will also ask unanimous consent to put in the record, we went up and looked in Boston of where they have a demonstration project, and I think there is still one in Detroit, and we saw unbelievable configuration.

Chairman ISSA. Without objection.

Mr. MICA. And we want to detail our findings, which we also passed on to the administration.

Chairman ISSA. Without objection that will be placed in the record.

And I now go to Mr. Boswell, a gentleman who I served with on the Select Intelligence Committee, who more than anybody here on the dais today knows what the special skills are necessary to read somebody who may be a terrorist. And the gentleman is recognized.

Mr. BOSWELL. Thank you, Mr. Chairman. You may have overstated that a little bit but nevertheless.

Chairman ISSA. No, I remember our times behind closed doors very, very well, and you were truly the senior statesman there on that issue.

Mr. BOSWELL. Very, very kind, and I appreciate it. First off, I want to start with a positive remark. We stood up what we do, Mr. Chairman, is going to be a pretty humongous agency, as we started out with the need we had and the situation that caused it. And I would like to compliment the courtesy and the efforts that people starting new careers, if you will, have demonstrated.

The one thing that amazes me, and it is not rocket science, and I have been waiting and waiting and waiting; I was really pleased to see we could realize we could push the air crews through a little quicker and not delay things. There are a number of us here, myself included, that held probably as high a clearance as one can get for years, but I still am checked as if I were suspect of walking through the same airport, time and time and time and time again.

I know there are some people that have a malady because of things happened in the service. And there seems to be no effort to recognize that, my gosh, they have had a background check, top secret, top secret crypto, so on and so on. Do you have any intention to ever try and take advantage of that and expedite things a little bit, or are you going to keep on doing it like you have been doing it?

Mr. McLAUGHLIN. Sir, actually, the answer to that question is we are actively engaged with a number of different groups to try to expand our PreCheck population. Again, PreCheck is the program that is allowing expedited screening for individuals that are qualified, either today in pilot phase because they are part of frequent flier program or they have opted in through CBP's Global Entry.

We extended the program to active duty military traveling out of Reagan National airport. That started last week.

And we are exploring other groups that we can work with.

Mr. BOSWELL. Well, I understand the active military, and you know, people like Mr. Issa and myself and others, you know, took off the uniform one day and did work the next, but the history is still there.

Mr. McLAUGHLIN. We are actively looking at that.

Mr. BOSWELL. What is your timeline for active on this? Seems like simple, straightforward; the record is either there or it is not. The case that I know of, at least I can speak for myself, I know the record is there.

Mr. McLAUGHLIN. There are two aspects, really, that we focus on.

One is, to your point, if the record is there, and then two is our ability to reconcile that at the checkpoint. So there is a technology piece that allows us to verify that someone is who we believe they are.

We started this process in the fall of last year, and already, in just March, we are up over 600,000 participants in the program. So I think we are working quickly to expand the program, but we are doing it also cautiously to make sure that we are maintaining security every step along the way.

Mr. BOSWELL. I appreciate that, but I still just don't understand why you can't take—it is like discovering the wheel all over or passing up the fact that we have spent a lot of money in the past on doing background checks on a number of people, and it is just like it never happened.

How many years have been going on now that we have been doing this? And it seems like you have had time to proceed a little bit further along the way. But, again, I want to leave and stop on a positive note. I think that the personnel are courteous, work hard and are sincere and are following the rules that the administrators gave them to operate by.

I just think we could do a little bit better. I do appreciate the fact we don't have to leave pilots and air crews standing in line as we did for some time. I thought that would probably get solved, but we are leaving a lot of other people. It takes up time. It clogs up the process when it could be a pretty simple identification. Most of us that have spent time in the service have even got a printed ID

card that says we served 20-plus years, and a lot of information on there, seems like it could be used.

Thank you very much, Mr. Chairman.

I yield back.

Mr. FARENTHOLD. [Presiding.] I see I am up next. So I will yield myself 5 minutes.

First off, I would like to thank you all for taking the opportunity to be here. I think I am in the unique position of being the one Member of Congress who actually serves on all three committees that has jurisdiction over the TSA: Government & Oversight Reform Committee; the Transportation Committee; and Homeland Security. So I actually spend a whole lot of time with this issue, as well as quite a bit of time traveling and experiencing the service of the TSA.

I would like to say the vast majority, I would say almost without exception, but there are exceptions, the TSA employees that I have encountered in my travels have all been courteous and professional in nature.

However, as part of preparing for this, just like Chairman Issa, I opened up my social media sites to comments with respect to experiences with the TSA, and I received quite a few negative comments as well.

And without objection, I would like to get those entered into the record as well. So ordered.

Mr. FARENTHOLD. I do want to talk about some of the problems that people have reported with the TSA. I understand we are in a situation where it is a stressful environment for many people traveling. The TSA is squeezed into spaces in airports not designed for the level of screening, but if you look at some of these instances, and we had one in the news just last week of the gentleman in the wheelchair being patted, it seems like at some point if we could just use some common sense and slow down a little bit and offer to do some of these screenings in a private area or in a screened-off area. And maybe it is worth spinning a little effort on creating spaces that are a more friendly to that; we might be able to do better there. I just encourage both the TSA and the traveling public not to get worked up. I think there are some better ways to do this.

I did want to talk a little bit about the SPOT program. I am concerned how effective behavioral detection program is with the limited amount interaction there is between the TSA agents and the general public. About 6 months ago, I think I commented in one of these hearings that I could get through the entire airport without uttering a word other than "thank you" to anybody: Check in at a kiosk; hand my stuff to the TSA; hand my stuff to the gate agent. Now at least the TSA is at least asking me for my full name.

It seems like SPOT would be better off if there was a little bit more engagement.

Mr. McLaughlin and Mr. Sadler, would you like to comment on that.

Mr. McLAUGHLIN. Thank you. First, if I could, just for everyone's awareness, every passenger that travels through checkpoint is entitled to private screening upon request. We want to make sure that we honor that commitment.

Mr. FARENTHOLD. It might be something you consider offering, especially to the elderly and disabled and children.

Mr. McLAUGHLIN. Sure. And with regard to the video from last week, that was actually a video that was over 2 years old. And with the policy changes that we put in place last fall, again, we have seen a traumatic decline in the number of times where we have had to pat down children and now the elderly with our new program.

With regard to SPOT and your question, sir, I agree with you that our SPOT program in its current form is largely an observation program where our officers are trained to observe signs of fear, of deception, and of stress that are different than the general traveling public—

Mr. FARENTHOLD. And Mr. Lord, there is no way to really test that, because you can't imitate those behaviors. Is that correct?

Mr. LORD. While the behaviors can be imitated, as in any deterrence program, it's effectiveness is difficult to evaluate.

Mr. FARENTHOLD. I apologize, I am going quickly because of time. What is the roll out schedule nationwide for TSA? I dusted off my Global Entry card because I am looking real forward to being able to use that.

Mr. McLAUGHLIN. We have, the administrator and the Secretary announced I think in February that we intend to roll out to the 35 busiest airports by the end of this calendar year. And so far, we are on target for that. As of last week, we are at 11 airports, and we continue to roll out a couple airports a week and will begin adding additional airlines as well.

Mr. FARENTHOLD. Mr. Lord, I know you spend a fair amount of time studying what the TSA does, and I have also had access to some of these classified reports to a level that I am a little bit concerned. But I wanted to ask you, do you see some things that we are not doing that we should be doing to increase security? I know that really isn't something specifically you study, but you all spend a lot of time looking at what they are doing and how.

Mr. LORD. I can't think of anything off the top of my head. We completed a large body of work on various layers of TSA's security programs. All of our reports include recommendations to improve things, so we think we are having a positive impact on the programs, and TSA has been very receptive to most of our recommendations.

Mr. FARENTHOLD. I see I am out of time. Hopefully, we will get to a second round of questions. I will now recognize Mr. Connolly, the gentleman from Virginia, for 5 minutes.

Mr. CONNOLLY. Thank you, Mr. Chairman. And thank you all for being here today.

I think we need to start, as our colleague Mr. Boswell did, positively recognizing the extraordinary difficulty of the mission here. In a free society, how do we graft on to that protective and necessarily often intrusive measures to protect the public, after tragedy of 9/11 especially? In a democracy, frankly, it seems to me we ought to be arguing about this all the time, because I don't think we should ever get complacent about either side of this, my right to privacy and my right to be protected, and the role of government in fulfilling that mission.

So I think it is a natural tension and not necessarily always a reflection on the men and women who are trying to fulfill this mission.

And my observation thoroughly is that the men and women who have been recruited to fulfill this mission are actually doing on balance, a very good job. And many of them are very professional in their approach to the public. But as the chairman indicated and Mr. Issa indicated, our committee chair, there are, however, occasions where that is not the case.

And one thing I just commend you, Mr. McLaughlin, and you, Mr. Sadler, a simple training in “please” and “thank you” would really go a long way with the public. I wish I could say everybody remembers that, but we are not cattle, and we are citizens, and we are not to be presumed guilty of anything. And barking orders like people are cattle is not appropriate. And I would urge you strongly to make sure—I know it seems simple, but it gets on the traveling public’s nerves, and it undoes a lot of the wonderful work otherwise being done by the employees of TSA.

So, once in a while, there are people who just, I don’t know, they don’t feel they need to do that or they are giving orders. And what we are really trying to do here in a free society is to get compliance. And most of the public I think actually understands that and is willing to tolerate the fair amount of intrusiveness, more than I would have guessed actually, but they do expect to be treated with respect.

So I think so long as we can do that in the training of our men and women, I think we would also go a long way to enhancing the compliance, understanding we are all in this together.

Mr. Lord, last year, TSA ranked 232 out of 241 Federal agencies and entities in the Partnership of Public Services Best Places to Work. In other words, it was in the bottom 5 percent of Federal agencies as, yeah, I would love to work there. And it ranked second to last for pay, family-friendly management policies and performance-based incentives. Would you comment?

Mr. LORD. I am aware of that survey. First, I would like to comment that GAO consistently ranked near the top. I believe, last year, we were second.

I saw the scores for DHS and TSA. I think some of that reflects, they have a very large screening workforce that does a somewhat stressful job. They are interacting with the public on a day-to-day basis, and sometimes that is stressful. It wasn’t clear to me, though, what the department was doing about it on an organizational wide basis.

Mr. CONNOLLY. We are going to give them an opportunity to comment on that. But are you familiar with the turnover rate last year?

Mr. LORD. Not specifically.

Mr. CONNOLLY. Would it surprise you for me to tell you that it was 13 percent?

Mr. LORD. If that is accurate, that would not surprise me, no.

Mr. CONNOLLY. And it has been 10 percent for at least the last 5 years and that that is significantly higher than the average of Federal agencies?

Mr. LORD. Any time any organization experiences that type of turnover, obviously, you are dealing with some—it imposes certainly challenges—

Mr. CONNOLLY. Given the sensitive nature of the mission, the security mission, should it concern us, in your opinion, that we have low morale and high turn over, and that that actually could—in theory, could affect the performance of the mission?

Mr. LORD. I am not sure what the root causes are.

Mr. CONNOLLY. Well, putting aside causes, just those facts, would that not suggest it could compromise the mission, that we are less than enthusiastic about carrying out the mission or less than caring about it because I don't even like being here. I don't like my boss or I don't like the policies of the agency. What I am worried about is, in addition to the men and women who are suffering that low morale, what is the impact on the traveling public in terms of their carrying out their mission?

Mr. LORD. That would concern me as a TSA executive.

Mr. CONNOLLY. Mr. Chairman, I won't ask any more, but if you would wouldn't mind allowing Mr. McLaughlin and Mr. Sadler to respond.

Mr. FARENTHOLD. Without objection.

Mr. CONNOLLY. I thank the chair.

Mr. McLAUGHLIN. Thank you.

First of all, to your comment about training, I am pleased to let you know that earlier this year, we began a training initiative that we are referring to as PACOM. And that initiative is a training that all TSA frontline employees and their managers in the field will go through, which focuses specifically on active listening skills, on empathy, as well as on a communication technique that hopefully will improve that experience; the caveat being that airports are very busy and loud places, and sometimes it is hard to balance the need to communicate in a way that is heard without being overheard, so to speak.

My numbers with regard to attrition—

Mr. CONNOLLY. If I could interrupt you. There is a difference between, “please put your hands up,” you know, in the machine versus “put your hands up.”

Mr. McLAUGHLIN. Agreed and that is what this training addresses specifically.

Again, we are on target to get that training complete for managers and supervisors by June of this and for the entire frontline staff by December of this year.

The numbers that I have for attrition are 6.1 percent for full timers and then 18 percent for part-timers. So while we are concerned about the part time number, the overall number that I think you have might be skewed somewhat by that data.

With regard to what we are doing to improve our standing in the best places to work, and I can tell you from personal experience, first of all, being an employer in both the private sector and now in Federal service, having worked with thousands and thousands of employees, I will tell you that I am very proud of the dedication of my workforce and their commitment to the mission.

I think, overall, their focus on the mission is not consistent with the rating that we received in the best places to work. That being

said, we have a number of initiatives as we move forward to improve the overall morale. We have national advisory councils. We have trainings, like the ones that I described, where feedback from officers are—literally one officer described it as life-changing event for her in terms of her understanding of her role and how she could interact better with customers, which has an impact on morale.

And then I would also say some of it just comes with the newness with our agencies, an agency that is less than 10 years old or just now 10 years old is going to have a different growth curve than a Federal agency that has been around for 50, 100 or even 200 years.

Mr. FARENTHOLD. Thank you very much. We will now proceed to another expert in the field, the gentleman from Minnesota, former airline pilot himself, recognize Mr. Cravaack for 5 minutes.

Mr. CRAVAACK. Expert? I don't know about that. End user, yes, definitely.

I just have a couple of questions. And I thank everybody for coming here today because I think everybody wants the same issue, wants safety in the air, and make sure our people that are working with us are happy and do their job efficiently and effectively.

And thank you for the Coast Guard and all the things your men and women do for you, Admiral.

I would just like to talk about a couple of things. Joe passenger walking through my first level of security; I am going to go through SPOT. I see SPOT developing probably into something more of what we see in Amsterdam, Israel, going through more proactive challenge-reply, taking a look at behaviors. So I see that developing. Right now, it is not a totally effective tool, but let's just deal with the now if we may.

So we hit SPOT as we head on to the screening area. Go to the screening area, and Mr. Lord, you said 30 percent are used by AIT machines; is that correct, 30 percent of the passengers going through?

Mr. LORD. It is—yeah, according to Mr. McLaughlin, that is correct.

Mr. CRAVAACK. We found that some AITs were used less than 30 percent of the time, as highlighted in my prepared statement. So 30 percent of the passengers are going through the newer, more improved AIT machines. Would you consider, as much as you can within this arena, are the AITs 100 percent absolute? Are they fool-proof?

Mr. LORD. I can't discuss any of the details, but in general, any technology has limitations.

Mr. CRAVAACK. We all have limitations, any technology is going to have some type of limitations. Now, of course, through the metal detectors, those are a little bit less advantageous. So only 30 percent of those people have gone through the first phase of SPOT, now going through 30 percent will even say they go through an AIT machine, where the other 70 percent have gone through metal detectors, which are basically less—I don't want to say less safe, but not as good as the AIT machines.

Okay, then we get to the gate, and we have the gate agent making sure you get on the right aircraft. We have gone through some

security, but there is a possibility that something could have slipped through.

Let's talk about the aircraft itself. The aircraft is sitting on the tarmac, and around the aircraft, we have nearly a million airport workers working around that aircraft are credentialed. These credentialed airport workers have direct access to nonpublic areas and sanitized areas SIDs, so here they are working in the shadow of the air plane, close to a million workers. Could you tell me how these workers, these million workers, are credentialed?

Mr. LORD. There is a—they all are required to wear secure identification display badges, and they are essentially vetted against terrorist watchlists, immigration databases and criminal records.

Mr. CRAVAACK. We have all seen most recently with all of the—we have seen drugs being smuggled on board aircraft; we have seen numerous theft rings that have been working in and around the aircraft. And it would be safe to say that there are also holes within this program as well. Would you be correct in that?

Mr. LORD. There are various vulnerabilities in the layers based on the work we completed to date.

Mr. CRAVAACK. So we have a potential going to the aircraft, some passengers being screened, even having a very good possibility of getting through SPOT and also screening techniques. And we have just as equal opportunity for the potential of items being given—put on board the aircraft on the shadow of the aircraft through credentialed workers. So my question to you, and I am going to give you a very good one, Mr. McLaughlin, if you don't mind, sir, and I say this with all due respect, so with the potential of having a person that has malintent coming on board the aircraft, linking up with a device that is on board the aircraft through a credentialed person in the shadow of that aircraft, that aircraft gets underway and is in the air, what are the line of defenses capable in the air at that time? Who is the last line of defense, Mr. McLaughlin? And don't say the cockpit door, the armed cockpit door.

Mr. MCLAUGHLIN. That wasn't even my answer.

With the multiple layers in place, there are on a number of flights, we do have Federal Air Marshals. But the layer of security that is in place, that is an important layer today, and we talk about it from time to time and we know it when we fly, is the actual passenger. That individual that learned as many lessons on 9/11 as the rest us have learned.

Mr. CRAVAACK. True, no truer words are spoken. If I may have indulgence, Mr. Chair, but if a professional terrorist has done this routine a hundred times, they know when that cockpit door is going to be open. They know when it is going to be closed. They know a lot of things about the aircraft that your average traveling public does not know. So my question to you, sir, is there are really not that many FAMs available per flight, and that is a classified number, but why in God's green Earth would we cut in half a volunteer program that protects the aircraft for \$15 a flight? Why would we do that?

Mr. MCLAUGHLIN. Sir, I can't really discuss that topic because it is really outside my area of responsibility at TSA. I can reinforce some of the other layers that are on the ground, including the work

that we do in and around the airport, and we can take that question for the record in terms of—

Mr. CRAVAACK. I would appreciate that. This program, the Federal Flight Deck Officer program, is being cut in half, a \$15-per-flight program that was the last line of defense for many potential terrorists wishing to take that aircraft and use it as a weapon of mass destruction. So with that, sir, I would appreciate your information on that.

And with that, sir, I thank the chair's indulgence, and I yield back.

Mr. FARENTHOLD. Thank you very much.

We will now recognize the gentleman from Tennessee, Mr. Cohen.

Mr. COHEN. Thank you, Mr. Chairman.

First, I would like to incorporate by reference all the nice things said about TSA personnel in my home community in Memphis, particularly, for they be voters, but also in Washington, where they are not, have all been courteous and nice folk. They have got a tough job, having to do kind of a monotonous gig, and they are not the most popular people to see when you have to go through that. It is not like Customs and checkpoint Charlie, but still, it is something you don't look forward to and relish.

The other is about the TWIC cards, and I reiterate the concerns we have got in Memphis with the TWIC cards and they are important, but there seems like there could be a better way to allow the people that receive them to pick them up, rather than have to do it personally; they could be done through the mail like driver's licenses and other licenses are. An improvement in that system would be helpful in my community. Who is the expert here on the process we go through at the airport?

Mr. MCLAUGHLIN. The airport would be myself.

Mr. COHEN. Let me ask you this, today, for the first time, I was asked to take off my watch. Why?

Mr. MCLAUGHLIN. While I clearly wasn't there with you, it is possible that our divest officer, the individual who is working to facilitate the travel of customers, might have felt that it would alarm and that you might have had an easier experience by removing it, but you are not required to remove your watch.

Mr. COHEN. Well, they made it like everybody was; she was announcing, take off your watch. And just like with the very flawed systems that they have for onboard diagnostics and the check engine light and folks being able to get their car inspected, if the light is on, even if the car doesn't emit any type of carbon vapors over and above what is expected, they won't pass you. And they say, well, it will save you problems in the future. That is not EPA's job; nor is it your job to make it less likely.

I don't get it. It made no sense to me at all. And she said, you have got to take it off. I mean, it is just like, the rules need to be consistent. For a while, we didn't do shoes, and then the guy had the shoe, and then some places had shoes and some didn't. Now, today, I notice shoes must not be in a bin, but they must be laid flat on the conveyer belt. Is that a uniform rule?

Mr. MCLAUGHLIN. That is not a rule in place today. At one point, we actually changed our procedure with shoes and have subse-

quently some time ago changed that back to allow them to be placed in a bin or on the belt. However—

Mr. COHEN. In Memphis, they have got a sign that says they must be placed flat on the conveyer belt, which is not a big deal, but sometimes your shoes can get crushed between two bags. And if you care about your shoes, that is not wonderful.

The watch thing just seems it is the inconsistency of everything gets you. I am comfortable in my manhood, and so the guy was fine, didn't have a problem. But I got out, and he wanted to pat me down, and he patted down my chest. The same soap I use every day. Never been patted down before on my chest. The machine must have messed up is all I can figure.

Mr. McLAUGHLIN. Again, I can't speak to your specific situation, but I can look into it for you.

Mr. COHEN. I am not terribly concerned. It just seems like there should be some consistency. And the machines sometimes may be set at different levels or something, because sometimes you go through and they want to look at your arm or look at this or that. And I mean, I am not the Bionic Man in any—well, whatever. I don't have any parts that are new or metallic, so it makes no sense.

Mr. McLAUGHLIN. So our goal is to be uniform and consistent, and at the same time, we also want to be random and unpredictable at times because we find that is helpful in terms of our work in security, but we are looking for a uniform and consistent experience for travelers as they come through, and as I said, I am happy to follow up on that.

Mr. COHEN. I agree with Mr. Boswell that there probably should be some type of system where you have your most likely people that you know that are frequent fliers and are safe and going to do any—one day, there was this lady there who has got the richest husband in town almost. And she has got a place in Aspen, and she has got a place in France. And they were going through all of her—if anybody wants to stay alive, it is her. I mean, she has got it all. And they were going through all of her stuff. When they saw all of that, they should have realized, this woman wants to live. Sometimes it is a little common sense.

How much did the puffers cost us? The whole puffer process?

Mr. McLAUGHLIN. So the puffers predate my time at TSA, I can take that question for the record and get back to you. We talked earlier about the disposal fee for the puffers.

Mr. COHEN. And they are history, I know that, but that was a loser from jump street, too. I mean, here in Washington, one line had a puffer, and one line didn't. So if you are a terrorist, you would go through the line that didn't have the puffer, thinking the puffer worked. The fact that the puffer doesn't work, the terrorist could have chosen either line. But they said, well, extra security was given on the other line if there was some problem; they looked at you even closer. Well, if they looked at you closer in the other line, why didn't they look at you closer in the puffer line? I mean, the puffer thing was really bad.

But otherwise, all the TSA people are great. You have a tough job. I know you will make it better.

I yield back the balance of my time.

Mr. FARENTHOLD. Thank you, Mr. Cohen.

And the staff informs me that the puffers were around \$30 million. If that is incorrect, please let us know.

I think the same situation exists today. I fly home sometimes on American, sometimes on United. If you go on United at DCA, you go through a full body scanner. If you on American, you go through a metal detector. It doesn't take a rocket scientists to figure out there is a potential issue there.

We now recognize the gentleman from North Carolina, Mr. Coble.

Mr. COBLE. Thank you, Mr. Chairman.

I arrived a bit delayed. For that, I apologize; I had a conflicted schedule. And maybe these questions may have already been pursued.

Mr. Sadler, what has been the total cost of the TWIC program to the Federal Government and the private sector?

Mr. SADLER. To date, the program costs are approximately \$374 million. That would include \$100 million in appropriations and about \$274 million in user fees for individuals who have paid for the TWIC card.

Mr. COBLE. The Federal Government and the private sector, both?

Mr. SADLER. Yes, sir. That is the appropriated money to start the program, the \$100 million, and then the \$274 million was the user fees when you enroll and get a TWIC card issued to you.

Mr. COBLE. Thank you, sir.

Admiral, what is the amount of money that you allocate for TWIC administration each year?

Admiral ZUKUNFT. Ours is very minimal. We have expended about \$2 million looking at mostly commercial off-the-shelf technology.

Mr. COBLE. That is \$2 million annually?

Admiral ZUKUNFT. To date. That does not include the day-to-day expenses of our personnel. I do a number of missions, one of those is validating TWICs at these facilities, but that is part of our mission set already.

Mr. COBLE. And how many Coast Guard personnel are dedicated to oversight of the TWIC program?

Admiral ZUKUNFT. They are not dedicated solely to TWIC, but they do facility inspections. And TWIC is just one element of that. So they are looking at everything from what infrastructure is in place and so those exist at all of our sectors, all of our ports throughout the United States.

And one example of that is we recently shut down a facility in Miami because it didn't have the appropriate safeguards, unrelated to TWIC, but there were literally holes in the fence line that would allow people with no business to enter into those facilities.

Mr. COBLE. How long has TWIC been online?

Admiral ZUKUNFT. TWIC was implemented in 2009, on April 15th, and that is when 2,700 facilities were required to have TWIC. And on that milestone date, all facilities were in compliance. The TWIC reader is going to be critical as we go forward, because that will be the next enabling mechanism because that biometric chip is really what provides the next level of security, beyond the visual recognition that is on the existing TWICs.

Mr. COBLE. Thank you, Admiral.

Thank you, gentlemen.

I yield back, Mr. Chairman.

Mr. FARENTHOLD. Thank you very much.

Seeing no one else on the other side, I will go to Mrs. Blackburn from Tennessee for 5 minutes.

Mrs. BLACKBURN. Thank you, Mr. Chairman, and I thank the committee for allowing me to participate today.

This is an issue, TSA and their participation and their conduct is something that is important to my constituents. And Mr. Lord and Mr. McLaughlin have both mentioned constituent satisfaction, customer satisfaction, as a goal.

I would just commend to you looking at The Economist magazine's online poll, which they have up right now. And the question they are asking is whether or not changes made to airport security since 9/11 have done more harm than good. And at last check, as I checked, it was 87 percent of the readers agree that changes that airport security have done more harm than good.

So, gentlemen, I would contend that we are not doing our best at customer service, and I think, Mr. Connolly, my colleague from the other side of the aisle, spoke well to that.

I want to talk with you a little about the VIPR teams, because on October 20th, 2011, my home State of Tennessee became the first State in the country to deploy VIPR teams simultaneously at five weigh stations and two bus stations. The teams included your TSOs, BDOs, explosive detection, canine teams.

My office was informed by TSA that the point of operation was for TSA agents to recruit truck drivers into the First Observer Highway Security Program. The TSOs and the BDOs involved in the operation were only supposed to be handing out recruitment brochures since neither position has actual Federal law enforcement training. However, I have got a couple posters here; you can see back here. If you look at these posters, and I will call that one Exhibit A, and if you were watching the video of this transaction, you would see that this individual, who is designated as a TSA employee, is walking around and inspecting the truck. So if they were supposed to be handing out brochures, what were they doing inspecting the truck? And what type training do the TSOs and the BDOs receive to detect abnormalities or potential threats in semi trucks, Mr. McLaughlin?

Mr. McLAUGHLIN. Thank you.

First, the exercise—or I should say, the VIPR that you reference in your State of Tennessee was, it is important to note, a joint training exercise with 23 different agencies, both Federal, State and local, where TSA was invited to participate. And by all accounts, the 2- or 3-day exercise went off very well. It was an important opportunity for us to build relationships to ensure that in the event of a real national security emergency, we have the types of relationships—

Mrs. BLACKBURN. Sir, you are using my time. But I would just ask what type training do they have to actually do these inspections and to detect the abnormalities that would be there on our Nation's highways? Because they have no Federal law enforcement training, correct?

Mr. McLAUGHLIN. During this exercise, the officers did not conduct any screening of any vehicles, nor—

Mrs. BLACKBURN. Okay, let me put up poster number two. Then why did they ask to open the top of this—open this truck and look? Was there a specific threat to Tennessee highways on October 20th, 2011? And was there any intelligence suggesting that a suspected terrorist may be driving a semi truck across Tennessee? And were there specific threats that were deterred by conducting this operation?

Mr. McLAUGHLIN. Well, I can't talk about threats that might have been deterred. I can tell you, again, that this was a training exercise, not an exercise based on active intelligence in the State.

Mrs. BLACKBURN. Okay.

Mr. Sadler, do you have anything to add to that?

Mr. SADLER. No, ma'am.

Mrs. BLACKBURN. You don't. Well, there, again, I want to go back to this question, what kind of specific training do they have to be on the Nation's highways conducting these kinds of searches?

Mr. McLAUGHLIN. TSOs and BDOs do not receive specific training with regard to screening vehicles in the highway mode of transportation. The canine team that I believe that I see up there, although it is from a distance appears, to be a multi modal dog that is trained in that mode of transportation.

Mrs. BLACKBURN. So, even though our TSOs have no Federal law enforcement training, you are pleased that they you are participating in these type exercises?

Mr. McLAUGHLIN. Again, the VIPR program is set up to provide a visual deterrent and to work in conjunction with our State and local partners and all modes of transportation. And part of that, again, is to build relationships in terms of an exercise—

Mrs. BLACKBURN. So these TSOs, who have been administratively reclassified from being screeners and processors and given no Federal law enforcement training, are going to be out on our Nation's highways and our seaports and participating in this type of activity?

Mr. McLAUGHLIN. I am not sure I understood that as a question.

Mrs. BLACKBURN. Okay. Well, let me ask you this, based on the performance that you have seen with the VIPR teams and their ability to prevent specific terrorist threats, what kind of grade would you give them?

Mr. McLAUGHLIN. I think that our VIPR teams do a very good job in a mode of transportation where we have very limited resources. I think our VIPR teams working in conjunction with State and local agencies do a very good job of providing a visible deterrent to people that might be attempting to do something bad.

Mrs. BLACKBURN. A to F, what kind of grade would you give them?

Mr. McLAUGHLIN. I don't know that I have the experience to say specifically. Based on the experience I do have, I would give them a grade B plus to A minus, and that largely just based on the length of time that the program has been in place. It is a program that is only 5 years old in totality.

Mrs. BLACKBURN. I would just remind you that your agency has agreed that performance measures need to be developed for the

VIPR teams, so that there can be some measured results and some quantifiable data, and we will follow that as we move forward.

One last question that I would have for you, have the VIPR teams ever pulled over cars, SUVs or vans?

Mr. McLAUGHLIN. I am not aware of a TSA asset on a VIPR team pulling over a car or van, but I can take that question for the record.

Mrs. BLACKBURN. I would love to have that answer, because, to my knowledge, there is no terrorist that has ever driven a semi truck. So we find is very curious, the method that was being employed with the VIPR teams and their presence. And you can go look at the Zazi example or Shahzad example, and those were cars and SUVs. They were not semi trucks.

I yield back.

Mr. FARENTHOLD. Thank you very much. We will now start our second round of questioning, and I will give it a go for 5 minutes, and then we will go to Mr. Cummings.

As we talk about the SPOT program for a minute, if a BDO SPOT agent were able to see something that they considered to be suspicious behavior, what is the follow up there? What can they do? Do they engage the person in conversation? What is the procedure when a SPOT agent detects something? Is there something they can do? And if so, can you tell me what that is?

Mr. McLAUGHLIN. So, in our SPOT program, our officers are trained to observe behavior and engage in casual conversations with individuals. If the circumstances warrant, they can engage local law enforcement for further follow up.

Mr. FARENTHOLD. And so if they detected something suspicious, can they stop them from boarding the plane?

Mr. McLAUGHLIN. If you are asking can they physically detain an individual, SPOT officers are not trained nor do we want them to physically detain an individual.

Mr. FARENTHOLD. I set a SPOT officer off for some reason, and I can just walk on and get on my plane; they can't stop me.

Mr. McLAUGHLIN. I apologize. I misunderstood your question. I thought you speaking physically.

A SPOT officer, if they have reason to believe that you are suspicious, can engage a local law enforcement officer, who will interview you and either send you on your way or ask you additional questions.

Mr. FARENTHOLD. Has a SPOT officer ever stopped somebody from boarding a plane?

Mr. McLAUGHLIN. Not to my knowledge. Again, there are times when a SPOT officer will engage in conversation, but I cannot—I don't know of a time when an officer has stopped someone from getting an airplane.

Mr. FARENTHOLD. How much are we paying these guys to chat up passengers?

Mr. McLAUGHLIN. So our SPOT officers are paid in the same range as our Federal officers, beginning at the F band and topping G band, somewhere between \$37,000 and \$50,000.

Mr. FARENTHOLD. Last year, in TSA oversight, part one, hearing by the OGR committee, Chairman Mica asked some panels about the effectiveness of the full body scanners and whether or not they

could detect body cavity inserts or surgically implanted explosive devices. And the unanimous answer to that question was no.

On July 6th of 2011, the TSA released a notice to airlines warning them of the increased threat caused by explosive implant methods. And earlier this month, someone posted a video on the Internet demonstrating how to defeat these machines. Why are we continuing to spend hundreds of millions of dollars on technology with such obvious vulnerabilities? And what have you done with respect to the hearing last month and the revelation that they can't detect some these things?

Mr. McLAUGHLIN. First of all, I would point out that recently, our administrator testified with regard to AIT effectiveness. And there is a follow-up hearing, as I understand it, in the month of April in a classified setting where he will be able to get into more details. So I will tell you that we, obviously, on a daily basis review vulnerabilities in our system and ensure that we have mitigations in place, including AIT, which is our best deterrent or our best detection against metallic and nonmetallic threats—

Mr. FARENTHOLD. And is it your plan to replace all the magnetometers with AITs?

Mr. McLAUGHLIN. That is not our current plan. Based on sort of our evolution with the risk-based security, we are looking at the best way to deploy the best assets we have in configurations that makes sense across the system.

Mr. FARENTHOLD. And as they are purchased, are they getting deployed in a timely manner. I know there are some warehouses that a lot of this equipment sits in as it gets deployed, and the last I had heard, we weren't using modern deployment techniques, like drop-shipping them to airports.

Mr. McLAUGHLIN. To my knowledge there are no AITs in the warehouse that you refer to. The AITs are being deployed readily, and our utilization numbers are improving dramatically on a daily basis.

Mr. FARENTHOLD. And where are we with getting a peer-reviewed safety evaluation of these machines, specifically four TSA agents that are nearby and operating them and frequent screenees, be they frequent fliers or—I realize now the airline staffs are typically are diverted through magnetometers, but I saw a pregnant female TSA officer right by one of those machines and was concerned, because I understand there are no peer-reviewed safety checks there.

Mr. McLAUGHLIN. So with regard to the backscatter technology, which is the one that uses radiation, there have been three, as I understand it, independent studies, including one from NIST, one from the Food and Drug Administration, and one from the U.S. Army.

In addition to that, the machines are subjected to regular dosimeter testing to ensure that they fall within safe limits. And with every test that has been conducted, the units are well below established limits. All of the tests that I just referred to, both NIST and the Food and Drug, as well as the Army, and as well as the surveys with dosimeter surveys, are available on TSA's public Web site at [tsa.gov](http://tsa.gov).

Mr. FARENTHOLD. Mr. Lord, are you comfortable with those?

Mr. LORD. The IG recently reported on that and repeated much of the same information Mr. McLaughlin just provided. I am comfortable with what I heard, but if you are interested in having us conduct follow up, I can certainly talk to your staff after—

Mr. FARENTHOLD. Thank you very much. We will be in touch.

Now recognize the ranking member, Mr. Cummings, for 5 minutes.

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

Assistant Secretary Sadler, the GAO reported that its audit found that TSA had inadequate screening systems in place to identify applicants ineligible for TWICs and to deny the issuance of TWICs to them. What steps has TSA taken to address these findings?

Mr. SADLER. Well, the first thing we did was we created an executive level oversight board coordination with DHS to map out our short-term, medium-term and long-term strategy to address these recommendations. Immediately after receiving the report and the recommendations, we retrained the trusted agents; those are the individuals who collect the information at the enrollment sites, their ability to identify fraudulent documentation.

We also made system modifications that allow to us collect more information on the documents that are collected, pass that to our adjudicators so they could be reviewed more thoroughly. The mid-term and longer-term plan, we are making arrangements with the U.S. IDENT system, U.S. VISIT, so we can send our fingerprints into that repository and check our fingerprints that we have against the fingerprints in their repository to see if anybody is applying under multiple names or identities.

The other long-term project that we are working on is to wrap that capability with the FBI, and what that means is, currently, we are required to submit fingerprints, a new set of fingerprints each time we want a criminal history records check. What we are working towards is seeing if we can submit the fingerprints we have on file to the FBI to get a criminal history records check without hauling someone in to submit a new set of prints, and also that capability will tell us if the individual has committed some type of criminal offense in between the applications that they make every 5 years.

So there are a number of things we are doing. We took the recommendations very seriously, and we are doing the best we can with the program. We want to make it the best that it can be.

Mr. CUMMINGS. Now, during a hearing on TWIC held by the Senate Commerce Committee in May of 2011, Mr. Lord indicated in response to a question from Senator Boozman that a normal driver's license is at least as secure, probably in many cases more secure, than a TWIC. Is a TWIC more or less secure than a normal driver's license?

Mr. SADLER. I would have to defer to Mr. Lord on how he came to that conclusion. But for the TWIC, we think that TWIC is a secure credential, because you have to remember prior to TWIC, you could go to a port and gain access to a port with multiple credentials, possibly a credit card, a union card, any number of credentials.

So the first thing I would say about the TWIC is, it is the first time a common credential has been issued in a maritime environment, which means we can train to that credential. The second thing I would say is we developed many security features to put on that card, and we did that in coordination with other agencies, including the forensics document lab at ICE. So we did the best we could do make that card secure.

And then you also need to keep in mind it has a biometric on it, and although the readers aren't in place at the Coast Guard does have portable handheld readers that they can use to do random checks and security checks, as well as do checks as far as for port security inspections and vessel security inspections each year.

Mr. CUMMINGS. Admiral Zukunft, Section 809 of the Coast Guard Authorization Act of 2010 exempts mariners who do not need access to a secure area of a vessel from the requirement that they obtain a TWIC. Coast Guard Policy Letter 1115 implements Section 809 but still requires those seeking their first mariner credential to visit a TWIC enrollment center, essentially, to complete the TWIC enrollment process and pay the enrollment fee.

Admiral, I understand that the TWIC exemption has been estimated by the Coast Guard to apply to potentially 60,000 of the 210,000 licensed mariners in the United States. Is that correct?

Admiral ZUKUNFT. That is correct. And to date, we have only had approximately only 68 take advantage of the 809 provision.

Mr. CUMMINGS. And why do you think that is?

Admiral ZUKUNFT. For some, they see that TWIC as an employment opportunity. So if an employer would ask, why do you not have a TWIC, in this competitive environment, they see that as advantageous to have that credential and an up-to-date background check.

Mr. CUMMINGS. I see my time has expired. I yield back.

Mr. FARENTHOLD. Thank you very much. There are quite a few other questions, and some of the other members that had to leave did want to ask some additional questions, so with that in mind, we will be submitting additional questions in writing to complete the record as we finish this up.

Also, without objection, I would like to leave 7 days open for members to submit both those questions and opening statements.

I would like to thank each and every member of the panel for being with us, commend you for your service to this country, and urge you to continue to look for ways to improve what you and your agencies are able to do to better serve and better spend—more efficiently spend and use the taxpayers money to provide a safe transportation environment for all of us. Thank you for being here.

We are done.

[Whereupon, at 3:30 p.m., the committees were adjourned.]

GARRELL E. ISSA, CALIFORNIA  
CHIEFMAN

DAN BURTON, INDIANA  
JOHN L. MICA, FLORIDA  
TODD RIESSLI, PENNSYLVANIA  
MICHAEL B. TURNER, OHIO  
PATRICK MCHENRY, NORTH CAROLINA  
JIM JORDAN, OHIO  
JASON CHAFFETZ, UTAH  
CONOR RAOFF, FLORIDA  
TIM WALBERG, MICHIGAN  
JAMES LAMARCA, DELAWARE  
JURIN ABRAHAM, MICHIGAN  
ANN MARIE BUEHNER, NEW YORK  
PAUL A. BOSAR, ARIZONA  
RUBEN R. LADRADON, OHIO  
PATRICK MESHAN, PENNSYLVANIA  
SCOTT DUNBARLANI, M.D., TENNESSEE  
JOE WALTON, ILLINOIS  
TREY GOWDY, SOUTH CAROLINA  
DEWANE W. ROSS, FLORIDA  
FRANK C. GUINTA, NEW HAMPSHIRE  
BLAKE FANTHOLLO, TEXAS  
MARC GILLY, PENNSYLVANIA

LAWRENCE J. BRANDY  
STAFF DIRECTOR

ONE HUNDRED TWELFTH CONGRESS

**Congress of the United States**  
**House of Representatives**

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAKING 020 225-5074  
FAXING 020 225-3674  
HOURS 020 225-5051  
<http://oversight.house.gov>

ELIJAH E. CUMMINGS, MARYLAND  
RANKING MINORITY MEMBER

EDOLPHUS TOWNS, NEW YORK  
CAROLYN B. MALONEY, NEW YORK  
ELEANOR HOLMES NORTON,  
DISTRICT OF COLUMBIA  
DENNIS J. KUCINICH, OHIO  
JOHN F. TERRY, MASSACHUSETTS  
WM. LACY CLAY, MISSOURI  
STEPHEN F. LYNCH, MASSACHUSETTS  
JIM COOPER, TENNESSEE  
GERALD E. CONNOLLY, VIRGINIA  
MIKE DUBILEY, ILLINOIS  
DANNY K. DAVIS, ILLINOIS  
BRUCE L. BRALEY, IOWA  
PETER WELCH, VERMONT  
JOHN A. YARMUTH, WEST VIRGINIA  
CHRISTOPHER S. MURPHY, CONNECTICUT  
JACQUE SPER, CALIFORNIA

**Opening Statement**

**Rep. Elijah E. Cummings**  
**Ranking Member, Committee on Oversight and Government Reform**

**Joint Hearing of the Committee on Oversight and Government Reform and  
the Committee on Transportation and Infrastructure**

**“TSA Oversight Part III: Effective Security or Security Theater?”**

**March 26, 2012**

Today, the Oversight Committee and the Transportation and Infrastructure Committee convene to examine measures TSA utilizes to secure our nation’s transportation networks.

In the realm of aviation security, TSA must achieve a delicate balance. TSA must be effective in meeting the evolving threats posed by terrorists. We also expect it to be responsive to the needs of the public and the demands of commerce.

Since the terrible events of September 11, 2001, several attacks have been attempted against commercial planes, including the attempted bombing on Christmas Day 2009 of Northwest Airlines Flight 253, and the attempted bombing in 2010 of a cargo jet using a bomb disguised as an ink jet cartridge. These incidents demonstrate the constantly evolving threats TSA must counter.

TSA’s 43,000 Transportation Security Officers must screen more than two million passengers every day at our nation’s 450 airports. Although the vast majority of passengers pose no risk, these Officers must find the equivalent of the needle in the haystack.

In response to the Christmas Day bombing attempt, TSA increased its deployment of Advanced Imaging Technology systems to screen passengers for both metallic and non-metallic threats. More recently, TSA has developed the PreCheck program to expedite screening for low-risk travelers, such as members of the military. I welcome TSA’s efforts to develop a more intelligent, risk-based approach to transportation security.

Recognizing the enormity of the challenge TSA faces, as the agency develops new screening techniques, we must ensure that it strikes the appropriate balance between moving too

quickly to deploy untested or unreliable technologies or techniques and moving too slowly to address new threats.

Today's hearing will also review the Transportation Worker Identification Credential (TWIC). When I served as Chairman of the Subcommittee on Coast Guard and Maritime Transportation, I convened hearings in 2007 and 2008 to review the roll-out of TWIC, and I thank the Coast Guard for joining us today.

Unlike many screening techniques TSA uses in the aviation realm, Congress mandated what became the TWIC program and required that this program be funded by fees collected from enrollees.

There are now more than 2.1 million enrollees and, by our estimate, these enrollees have paid approximately \$280 million to implement this program. To close the security perimeter that TWIC is intended to create, we must finally implement the use of readers so these cards are no longer just expensive "flash passes." TSA must also ensure that TWICs are not issued to ineligible applicants.

However, we must also view TWIC in the broader maritime security context. TWIC is meant to control landside access to secure areas of U.S. ports and to secure areas of U.S. vessels. There are many risks that approach our ports particularly from the waterside that TWIC was never intended to address.

None of the individuals on the estimated 17 million small boats operating in our waters are required to carry TWICs, and none of the foreign mariners on the more than 9,000 foreign-flagged vessels calling on U.S. ports carry TWICs.

Our first and most critical line of maritime defense – our thin blue line at sea – is the U.S. Coast Guard, which must defend our coasts, rescue thousands at sea, respond to marine casualties and oil spills, intercept drugs and migrants, and enforce security requirements at 2,500 facilities and on nearly 13,000 vessels regulated by the Maritime Transportation Security Act.

This service of 42,300 active duty officers and members do all of this on a budget of less than \$10 billion per year – less than two percent of the DOD's base budget – and they now face additional cuts and the loss of up to 1,000 active duty slots in next year's budget.

The Coast Guard does all that we ask of it and more. However, we cannot continue to stretch this service and assume that it will never break or that gaps will not open in our maritime security.

**Facebook Questions & Comments for TSA**

*Bob West*

*Tallahassee, Florida*

Something needs to be done they are out of control.

*Pete Lowenstein*

*DeLand, Florida*

Yeah Congressman Mica, hang in there for us.

As for TSA, generally dealing with them as the unknown I am to them is a demeaning, insulting, aggravating experience & as if it's there just to give aggressive idiots full time jobs doing nothing but costing us regular people time money and temperament. Who has TSA actually apprehended & prevented from acting against we the people? Seems the TSA is against 'We The People' more than the people they allege to "protect us from". That my good sir, clearly fits the definition of an expensive, selective, false! Clearly, another tactless Goyt' stumble for us.

*Robin Mansfield*

*Key West, Florida*

Mr. Mica, Would you send your wife or daughters on a walk down a dark alley in the most vile ghetto drug infested crime ridden neighborhood? May as well just send them to the airport to be groped and robbed it that's case! I used to fly 2-3 times a month. When the TSA started rolling out the body scanners and grabbing "sensitive" body parts I had just had enough. I don't need some creep in some back room getting a peek at my nude body nor am I going to have some dirty blue gloved idiot grab my goodies while another is rattling around in my purse thinking about what item of value they want to take home! My God even if a person survives the humiliation and does not get something confiscated or stolen during screening they board a plane where a large majority of cargo right under their asses is not even screened! I've just determined the TSA is nothing more than a jobs program for a bunch of idiots that can't even get jobs gather carts in the Walmart parking lot!

*Matt Koegler*

*Enterprise, Florida*

My biggest problem with TSA is that it's pabulum to make the masses think something is being done to protect them.

*John Steele*

*Miami, Florida*

Want to reform TEA? Eliminate it entirely. Stop their intrusive, humiliating and unconstitutional activities.

*Ted Wolfe*

*DeLand, Florida*

I would like to know why a passenger has to go through all the hoops that TSA has created and then can go to a restaurant, within sight of the security gate (like at Midway Chicago) for breakfast, and be given a knife that could be a far more potent weapon than any of the stuff they made the passenger through away.

*Andrew Davis*

*Atlanta, Georgia*

Ask them about the pending lawsuit with former Congressman Bob Barr and Liberty Guard. Are they intentionally hiding documents?

*Ben Sauriol*

End the TSA! Stop the molesting of kids and disabled people. We cannot sacrifice liberty for security. If you do, you lose both. I'm in District 6, so please hear me on this.

*Ben Sauriol*

What does the CFR say about the TSA?

*Sara Nabozny*

Why does the TSA have the 3 oz toiletry rule? They can't enforce it, and it is a HUGE inconvenience - especially for women.

*Brenda Van Pay Steiner*

I don't think the issue is finding out information on the TSA's procedures... It should be abolished altogether. It should be the airlines responsibility to make travel safe, not tax payers. One more unnecessary government agency, that limits our freedom.

*Joyce Zarda Naps*

On a scale from 1-10. This is a -5 in importance!



**U.S. House of Representatives**  
**Committee on Transportation and Infrastructure**

John L. Mica  
 Chairman

Washington, DC 20515  
 November 8, 2011

Nick J. Rahall, III  
 Ranking Member

James W. Coon II, Chief of Staff

James H. Zeln, Democratic Chief of Staff

The Honorable John S. Pistole  
 Administrator  
 Transportation Security Administration  
 601 South 12th Street  
 Arlington, VA 20598

Dear Administrator Pistole:

As you know, the Government Accountability Office (GAO) and House Committees on Science and Technology and Transportation and Infrastructure have conducted reviews of the performance of TSA's Screening Passengers by Observation Techniques (SPOT) program. GAO and the House Science and Technology Committee found the testing of TSA's behavior detection operations failed both in performance and were inadequately constructed to detect behaviors that might indicate the passenger posed a threat and required additional security measures. As a result, GAO confirmed that TSA failed to detect 17 known terrorists that flew on 24 occasions, passing through security at eight SPOT airports.

With TSA's current and ongoing efforts to revamp the existing behavior detection protocols, I, along with House Congressional investigative staff, reviewed the Boston behavior detection demonstration project. I was completely disappointed that very little thought or sophistication was apparent in the construct of this demonstration. Rather than employing several highly-trained transportation security personnel to observe and question select passengers, the demonstration project employed a large, bureaucratic ensemble of TSOs who expended an inordinate amount of time performing meaningless interviews with all passengers, regardless of risk level. When I questioned TSOs about their level of training and knowledge of techniques, it was apparent they had not received even minimal training or oversight from knowledgeable staff. It is difficult for me to imagine a more cumbersome, manpower-intensive and ineffective method of operations. None of the TSO deployed a risk-based assessment or utilized common sense in questioning of passengers.

When questioned about the protocol for additional screening of individuals who may pose a risk, a TSO informed us that travelers who are risk-identified would be screened by a metal detector and baggage screener. Even more egregious, their most sophisticated screening equipment, an Advanced Imaging Technology detector, was not in operation because the airport's TSA lacked sufficient numbers of trained personnel on duty. While it is bad enough

The Honorable John S. Pistole  
November 8, 2011  
Page Two

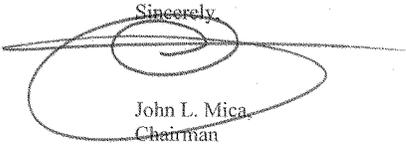
this demonstration is a costly and bureaucratic method of screening, it is completely unacceptable an operational model cannot be deployed in a manner that utilizes existing advanced technology and resources.

Once again, TSA's ineffective and costly behavior detection program appears to be headed in the wrong direction. Unfortunately, it appears TSA, whose budget has nearly doubled in the past decade and is now approaching \$8 billion dollars this year, has found another expensive and poorly conceived passenger screening procedure on which to spend taxpayer money.

Even with passenger screening checkpoints now sporting high-end U.S. flags with gold stands and with the replacement of white shirts with blue shirts and custom designed badges to make screeners appear more like law enforcement personnel. TSA continues to mindlessly spend public dollars.

If designed and implemented effectively, an interactive behavior detection program is an extremely valuable element to a risk-based security plan. TSA's current implementation of its SPOT pilot program is an unthinking, bureaucratic morass that treats all passengers as if they pose the same risk. I request that the TSA immediately halt the current SPOT pilot program until it can effectively incorporate an intelligent interactive representation of a behavior detection program where limited numbers of highly trained behavior detection officers observe and question selected passengers. A risk-based passenger screening system was promised with improvements in efficiency and performance and unfortunately it appears TSA is moving further from that goal.

Sincerely,



John L. Mica  
Chairman

Submitted for the Record by Rep. Farenthold

March 26, 2012

- Airbrushed Graphics: Why are non commissioned, non sworn officers allowed to put their hands on me and my family in that way, why are American citizens guilty until proven innocent? Q2 why do they site John Hopkins medical saying the body scanners are safe when John Hopkins themselves said that repeated or prolonged exposure to them is dangerous?
- Mark Paulson: Agreed on the scanners, we were subjected to 4 scans on our last trip, don't dig 'em at all!
- Gerald Reyes: I agree with the non sworn "officers" treating citizens as criminals first. It's becoming pervasive in America today. I should be able to travel with my lawful possessions and not have to answer how and why I have certain items that ARE allowed on a plane. I try to avoid flying. I don't want my daughter to think these questions and searches are normal in America just to go visit family.

Statement of Congressman Gerald E. Connolly  
Transportation Security Administration  
March 26, 2012

I appreciate the opportunity for the Oversight and Transportation Committees to consider the effectiveness of the Transportation Security Administration. A decade after Congress created the Department of Homeland Security (DHS), the agency is still on the Government Accountability Office's (GAO) high risk list. We need to drill down and identify which agency components are not performing as well as they could and how they can improve. However, what is not helpful in that endeavor is politicization of TSA management, such as the suggestion that its security program is "security theater."

Clearly, TSA management takes its agency mission very seriously. Its rapid deployment of creative and technologically advanced security measures demonstrates that the agency understands the threat of terrorism and the need to respond aggressively and proactively. It is appropriate that the agency is using both sociology and technology in attempting to protect American travelers from terrorism. While there are questions about the effectiveness of the Screening of Passengers by Observation Techniques (SPOT) and Advanced Imaging Technology (AIT), we should recognize that deployment of these techniques demonstrates the kind of proactive management that should be encouraged among agencies. It certainly is appropriate that we consider the effectiveness of these techniques and technology, but our review will be inaccurate if it fails to take into account the humans who implement these TSA programs.

On average, nearly one in ten TSA employees has left the agency each of the last five years. Last year its attrition rate was 13%, more than twice the average for federal agencies. In the Partnership for Public Service's review of agencies, TSA ranked 232 out of 241 agencies and components for best place to work. It ranked next-to-last for pay, performance-based rewards, and family-friendly culture and management. I know from my own constituents that TSA is a terrible place to work, and as a result many of them try to relocate to better-managed agencies or better components within DHS. This turnover rate makes it very difficult for the agency to maintain effective, highly trained screeners and undermines our national security. As the Partnership for Public Service notes, the costs of attrition are both monetary and operational. High attrition rates reduce productivity and forgo accumulation of institutional knowledge, weaknesses we can ill afford at important agencies like TSA. While I applaud TSA management for deploying advanced technologies to prevent terrorism, we expose our nation to great danger when we fail to maintain a stable, motivated workforce to conduct passenger screenings and other essential security work.

This Congress has only made the situation at TSA worse by freezing federal employee pay for multiple years and by attacking federal pensions. We cannot attract the skilled workers we need if Congress both denigrates the workforce at large and makes federal employment profoundly unattractive. We need to be fixing labor-management problems at TSA in particular while working to maintain competitive pay and benefits for the federal workforce as a whole. Only then can we be confident reforms to TSA screening techniques and other security measures will be effective.

<b>Question#:</b>	1
<b>Topic:</b>	AITs
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)
<b>Witness1:</b>	Chris McLaughlin – TSA Assistant Administrator for the Office of Security Operations
<b>Witness2:</b>	Steve Sadler – TSA Assistant Administrator for the Office of Intelligence and Analysis
<b>Witness3:</b>	Rear Admiral Paul Zukunft – USCG Assistant Commandant for Marine Safety, Security, and Stewardship
<b>Organization:</b>	U.S. Department of Homeland Security

**Question:** What metrics do you use to evaluate the security effectiveness, efficiency, and economic necessity of AITs? What metrics and criteria do you use to determine where to deploy AITs?

What is your plan for implementation of AITs? When do you expect to complete this AIT deployment? How many AITs will TSA procure in order to complete this deployment? How much will it cost to procure these AITs?

Please explain your progress in establishing a “roadmap” to help ensure AITs obtain higher detection capabilities.

Please make clear your efforts to provide more information to Congress about the results of these efforts.

Why did TSA deploy AIT units to locations where there is low passenger traffic?

**Response:** Many factors are taken into consideration before Advanced Imaging Technology (AIT) units are deployed, including airport readiness and checkpoint infrastructure. The Transportation Security Administration (TSA) performs risk assessments that analyze current threat information, detection capabilities of the AIT along with the other layers of security, utilization metrics, and the costs involved for both equipment and potential events averted. AIT systems undergo rigorous testing that includes both laboratory and field assessments for the evaluation of security effectiveness, efficiency, and suitability.

The AIT current Full Operational Capability (FOC) of 1,800 units may change based on the Transportation Security Administration’s Risk-Based Security initiatives, potential reductions in processing times, and qualification of new and innovative AIT solutions.

<b>Question#:</b>	1
<b>Topic:</b>	AITs
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)
<b>Witness1:</b>	Chris McLaughlin – TSA Assistant Administrator for the Office of Security Operations
<b>Witness2:</b>	Steve Sadler – TSA Assistant Administrator for the Office of Intelligence and Analysis
<b>Witness3:</b>	Rear Admiral Paul Zukunft – USCG Assistant Commandant for Marine Safety, Security, and Stewardship
<b>Organization:</b>	U.S. Department of Homeland Security

To date, TSA has received funding for 1,250 AIT units, of which 800 have been purchased. Of the units purchased, approximately 660 have been deployed to over 170 airports. The remaining units will be deployed through FY 2013. To reach the FOC of 1,800 units, TSA would need to deploy 1,140 more AITs and purchase 1,000 units at the cost (i.e., excluding installation, support, etc.) of approximately \$139 million to \$150 million.

On February 21, 2012, TSA issued a request for proposal (RFP) for a follow-on Advanced Imaging Technology (AIT-2) solicitation focused on the procurement of enhanced full size and reduced size AIT systems. The procurement specifications contained within the RFP for AIT-2 raise performance requirements in a number of areas to include reduction in processing time, increased detection performance, and reduction in size. The award date for full production is scheduled for March 2013 with all qualified systems from the solicitation configured with an Automated Target Recognition (ATR) capability, which produces a generic outline of a person to protect passenger privacy.

In collaboration with TSA, the Department of Homeland Security (DHS) Science and Technology (S&T) Directorate is also pursuing the development of an advanced AIT system with improved image resolution to allow for the detection of smaller threat items than currently possible with existing commercial systems. S&T is also pursuing development of next generation AIT systems that will allow a walk-through passenger screening process for anomaly detection, unlike the existing systems which require the passenger to remain stationary.

The Original Equipment Manufacturers with currently fielded AIT systems remain under contract with TSA to develop solution upgrades that include an ATR capability and incremental improvements in detection.

TSA will continue to provide regular updates to the House of Representatives and Senate, as well as congressional committees which have jurisdiction over TSA regarding AIT.

<b>Question#:</b>	1
<b>Topic:</b>	AITs
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)
<b>Witness1:</b>	Chris McLaughlin – TSA Assistant Administrator for the Office of Security Operations
<b>Witness2:</b>	Steve Sadler – TSA Assistant Administrator for the Office of Intelligence and Analysis
<b>Witness3:</b>	Rear Admiral Paul Zukunft – USCG Assistant Commandant for Marine Safety, Security, and Stewardship
<b>Organization:</b>	U.S. Department of Homeland Security

TSA will continue to provide information on procurement details, cost, schedule, associated staffing requirements, utilization rates, deployments, and progress on ATR development for Backscatter units and the deployment status of ATR.

AIT is the best technology that TSA has to detect both metallic and non-metallic threats on people going through a security checkpoint. Many factors, such as airport readiness and checkpoint infrastructure, are taken into consideration in determining where AIT units are deployed. As AITs are deployed to airports across the country, some will be installed at locations that have lower passenger traffic. This fact does not lessen the security benefit of AIT units.

<b>Question#:</b>	2
<b>Topic:</b>	SPOT
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

**Question:** What evidence/analysis does TSA have that demonstrates that SPOT benefits outweigh its costs, i.e., that the program is cost-effective?

The new SPOT pilot requires behavior detection officers to personally interact with passengers to help check out their “trip stories.” What have been the results of the pilot to date? What plans does TSA have to roll this out on a national basis?

When designing the SPOT program, did TSA consult with other government agencies such as the Secret Service, DoD, Customs and Border Protection, or the intelligence community?

**Response:** In April 2011, Department of Homeland Security (DHS) Science & Technology Directorate (S&T) completed a research study that confirmed that Screening Passengers by Observation Technique (SPOT) was more effective at identifying High Risk Passengers (HRP) than random selection protocols. Behavior Detection Officers (BDOs) serve as an important additional layer of security in airports by providing a non-intrusive means of identifying individuals who may pose a risk of terrorism activity. Currently, SPOT is one of the only scientifically validated behavior-based security programs in the world. TSA is conducting ongoing analysis to understand the cost-effectiveness thresholds for alternative concepts of operation and is working with DHS S&T to develop more definitive data on the probability of detection and probability of encounter of BDOs. Currently, the cost of BDOs in the field is approximately \$212 million for roughly 2900 Officers.

The Transportation Security Administration (TSA) is currently collecting data at Assessor pilot sites to evaluate the effect of enhanced behavior detection on security effectiveness, efficiency, passenger satisfaction, cost, and industry vitality. Assessor is a Proof of Concept program where BDOs apply the enhanced skills learned during Assessor training to evaluate whether passengers pose a potential risk to aviation security. The current concept of operations requires that Assessors perform document review and interviews with all transiting passengers, while observing for suspicious signs and behavioral anomalies at the Travel Document Checker (TDC) station. Based on the results of this engagement and observation, Assessors direct passengers to either standard or secondary screening. This is currently in operation at Boston Logan International Airport (BOS) and Detroit Metropolitan Wayne County Airport (DTW), and has been in operation since August of 2011. The evaluation strategy for determining effectiveness is similar to the DHS-sponsored validation study of SPOT conducted in April 2011, which

<b>Question#:</b>	2
<b>Topic:</b>	SPOT
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

examined the ability of SPOT to select potential high-risk travelers. Preliminary data reveals support for the pilot; however, additional data is required (and is being collected) to provide a complete analysis of the value of this new layer. Based on favorable results, TSA will continue to evaluate and develop a capability that captures both SPOT and Assessor qualities and create a comprehensive training package for the workforce.

The SPOT program was developed by TSA with assistance from the Massachusetts State Police (MSP). A SPOT working group was created in February 2004, comprising various TSA and Department of Homeland Security components (including offices of Civil Rights and Civil Liberties, Chief Counsel, Privacy, Policy, and the Transportation Security Laboratory), MSP, the Federal Bureau of Investigation's (FBI) Behavioral Sciences Unit, and the Federal Law Enforcement Training Center (FLETC). Additionally, members of the scientific community consisting of leading researchers in the area of verbal and nonverbal behavioral communication and deception detection participated in the working group.

<b>Question#:</b>	3
<b>Topic:</b>	BDOs
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

**Question:** What kind of training do BDOs receive before you qualify them to begin observing passengers for suspicious behavior? What metrics do you use to determine that this training course is sufficient to train a TSO to effectively observe behavior and appearance indicators in others? What kind of continuing training do BDOs receive each year?

**Response:**

*Initial Training*

All Behavior Detection Officers (BDOs) must be certified Transportation Security Officers (TSOs) before undergoing an interview process for the position. The TSO candidates must make the best qualified list locally after applying for the position, be interviewed for the position, and successfully pass the Screening of Passengers by Observation Techniques (SPOT) basic training course to become certified as a BDO. The SPOT basic training course is an eight day Instructor-led training course with four classroom days; one day allotted for end of course assessment and 24 hours of On-The-Job (OJT) training. For successful completion, the BDO must pass a multiple choice Job Knowledge Test (JKT) at the end of the classroom portion and meet standards/proficiencies of skills required during the OJT portion. Additionally, prior to becoming operational, the BDO must take required courses through TSA's Online Learning Center (OLC) that cover essential aspects of the BDO position.

*Metrics*

The metrics to measure the effectiveness of initial training are provided by the multiple choice JKT and the OJT Checklists. Subsequent assessments conducted during recurrent training and performance evaluations continue to measure knowledge and application of skills taught in classroom, online and on-the-job training.

*Recurrent Training*

BDOs are required to complete two kinds of recurrent training: Instructor-led and Web-based training.

BDOs attend a three-day Instructor-led SPOT Refresher course that provides an in-depth overview of the fundamentals of the job. This recurrent course is offered every 18 months and will be updated to reflect the most up-to-date procedures and behavior detection protocols.

<b>Question#:</b>	3
<b>Topic:</b>	BDOs
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

In addition to the instructor-led SPOT Refresher training, BDOs are required to take web-based, OLC courses. Web-based training courses can range from one hour to three hours in length. Some of the courses are required of all TSA personnel, while others apply more closely to the BDO position, including:

- Guidance Regarding the Use of Race for Law Enforcement Officers
- On Common Ground: Sikh American Cultural Awareness for Law Enforcement
- Arab American and Muslim American Cultures for DHS Personnel
- The First Three to Five Seconds: Arab and Muslim Cultural Awareness Training for Law Enforcement
- Introduction to Civil Rights
- Culture of Privacy Awareness
- TSA Policy on Employee Responsibilities and Conduct
- SPOT Recurrent Training Referral Report Form Tutorial
- SPOT Plain Clothes Operations
- Sensitive Security Information Awareness Training
- Risk Based Security
- Travel Document Checker

Moreover, the Instructor-led Additional Behavior Detection Training course provides supplemental training for BDOs in understanding how to conduct the Casual Conversation and direct their questioning based on behavioral indices, such as micro-expressions. This course can only be taken after the BDO has been operational for at least six months. A pre- and post-test was given during the pilot phase of this course to validate that learning had been achieved.

SPOT Transportation Security Managers are given all of the above training as well as an Instructor-led four day technical training course, Leading People and Managing Operations, which focuses on best practices for management within the airport environment, and administrative and communication skills.

<b>Question#:</b>	4
<b>Topic:</b>	TWIC 1
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

**Question:** Why has it taken ten years for you to meet your congressionally-mandated responsibility of developing and deploying TWIC card readers?

**Response:** A number of factors have contributed to the progress of the Transportation Worker Identification Credential (TWIC) reader deployment. To start, the Transportation Security Administration (TSA) had to resolve numerous policy and technological challenges, including testing reader and card technology at multiple maritime facilities nationwide and executing system design contracts for this first-of-its-kind program. TSA also had to develop card reader specifications that would meet maritime industry requirements for biometric identity verification, yet did not require a Personal Identification Number (PIN). Based on these factors, the first readers were not available for testing until July 2008, which accounted for a 15-month delay in commencing the TWIC Reader Pilot.

The TWIC Reader Pilot was the largest attempt, to date, to test biometric identity verification credentials and readers in a commercial setting. In addition to the delay due to the development of card reader specifications for the pilot program, and other pilot program preparations, TSA did not have authority over the pilot participants to expend TWIC pilot funds from FEMA, such as for awarding installation contracts. TSA's ability to influence the overall pace of the pilot and the level of resources participants applied toward pilot activities was limited; and the voluntary nature of participation coupled with competing local priorities and the economic downturn further slowed progress.

The U.S. Coast Guard (USCG) is evaluating the final pilot data as part of the TWIC reader rulemaking process. The next phase of the rulemaking is expected to be a Notice of Proposed Rulemaking. The USCG is required to review, analyze and take public comments into account before any final TWIC reader requirements can be implemented.

<b>Question#:</b>	5
<b>Topic:</b>	TWIC reader
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

**Question:** When will you satisfy your responsibilities to develop and deploy TWIC card readers? Please provide the USCG milestone chart regarding the TWIC program.

**Response:** The following comments summarize the actions completed to date and the milestones that lie ahead with this rulemaking project. The Coast Guard is diligently working to publish the Transportation Worker Identification Card (TWIC) Reader Notice of Proposed Rulemaking (NPRM). The Coast Guard published an Advanced Notice of Proposed Rulemaking (ANPRM) on TWIC reader requirements on March 27, 2009. In formulating the NPRM, the Coast Guard analyzed the public comments received in response to the ANPRM, as well as data from the Department of Homeland Security's TWIC reader pilot report mandated by the Security and Accountability for Every Port Act of 2006 and other sources.

It is difficult to predict exactly when the Coast Guard will publish the TWIC Reader Final Rule because the Coast Guard will be required to publish an NPRM, and then review, analyze, and take public comments into account before finalizing the rule. For this reason, the Coast Guard does not have a precise date for publication of the TWIC Reader Final Rule.

**Question:** Given that a TWIC reader costs several thousand dollars, and the additional costs of installing the necessary infrastructure and computer systems to support a TWIC-based access control system, how much of a financial burden will this program impose on ports and port facilities? How many readers will you need?

**Response:** The Coast Guard is currently collecting and analyzing available data to develop estimates of costs to install readers at affected Maritime Security Transportation Act-regulated vessels and facilities. Additionally, the Coast Guard is working with the Transportation Security Administration to analyze cost data from the TWIC Reader Pilot Program Final Report released on February 27, 2012.

The Coast Guard is using data from the TWIC Reader Pilot Program, along with other studies and reader vendor data, to estimate the costs to fully implement the TWIC program. Finally, the Coast Guard is diligently evaluating all available data before publishing a Notice of Proposed Rulemaking that will present estimates of the costs and the numbers of TWIC readers required at certain affected vessels and facilities.

<b>Question#:</b>	5
<b>Topic:</b>	TWIC reader
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

Until the Coast Guard has collected and analyzed all of this information, the Coast Guard is not yet certain of how much of a financial burden this program will impose on ports and port facilities, and not yet certain how many readers the Coast Guard will need.

**Question:** How do you expect to pay for the procurement and deployment of the readers?

**Response:** Owners and operators of certain Maritime Transportation Security Act (MTSA)-regulated vessels and facilities would be expected to pay for the procurement and deployment of the TWIC readers. MTSA-regulated facilities and vessels are afforded the opportunity to apply for funding for the procurement of these readers and related supporting infrastructure under the Port Security Grant Program.

<b>Question#:</b>	6
<b>Topic:</b>	TWIC 2
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

**Question:** What have you done to respond to the concerns in the May, 2011 GAO report regarding the security vulnerabilities that have resulted from your lack of developing and deploying TWIC card readers?

What has been the total cost of the TWIC program to the federal government and private sector?

**Response:** Since the Government Accountability Office (GAO) report was issued, the Transportation Security Administration (TSA) has continued its review of current internal controls with a specific focus on the controls highlighted in this report. TSA has held multiple meetings with the previously-developed working group to continue to document existing and in-development solutions to these recommendations. TSA completed a number of short-term actions to eliminate or mitigate many of the weaknesses identified in the report and continues to refine and track the progress of the longer-term solutions. As each of the long-term solutions progresses, TSA will continue to evaluate cost and schedule implications, in light of the anticipated Transportation Worker Identification Credential (TWIC) reader rule.

To date, the total cost of the TWIC program is \$356 million, of which \$264 million is TSA's cost (\$103M appropriated funds; \$161M fees) and \$92 million is the private sector contractor cost.

<b>Question#:</b>	7
<b>Topic:</b>	grants to ports
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

**Question:** DHS has awarded grants to ports for the purpose of procuring TWIC card readers. However, TSA has still failed to develop standards for these readers, and the grant money is about to expire. Will DHS extend the terms of these grants until TSA actually meets is congressionally-mandated requirements and sets standards for these readers?

**Response:** The Federal Emergency Management Agency (FEMA) is committed to all of its grantees to ensure that projects are completed and funds are spent for the purpose which they are intended. FEMA has worked closely with the U.S. Coast Guard (USCG) and the Transportation Security Administration (TSA) to provide grantees with the most flexibility, guidance and options for spending Transportation Worker Identification Credential (TWIC) related grant dollars. Specifically, FEMA published Information Bulletin No. 343 on June 21, 2010, that provided grantees the flexibility and options available to assist in executing TWIC related projects. In addition, FEMA has conducted extensive stakeholder outreach at conferences, with major port associations, and on a one-on-one grantee basis to assist with any issues concerning expenditure of TWIC awarded funding.

Should a grantee need a no-cost extension to its period of performance for a TWIC related project, FEMA stands ready to evaluate and approve such a request, based on the merits and justification of the request. FEMA will issue extensions, as appropriate, within the confines of the law.


**FEMA**

**Grant Programs Directorate  
Information Bulletin No. 343  
June 21, 2010**

MEMORANDUM FOR: All State Administrative Agency Heads  
All State Administrative Agency Points of Contact  
All Urban Areas Security Initiative Points of Contact  
All State Homeland Security Directors  
All State Emergency Management Agency Directors  
All Eligible Regional Transit Agencies  
All Private Sector Transportation Security Partners  
All Public and Private Sector Port Security Partners

FROM: Elizabeth M. Harman  
Assistant Administrator  
Grant Programs Directorate

SUBJECT: Interim Guidance for Ports, Facilities and Vessels on  
Transportation Worker Identification Credential (TWIC) Projects  
Funded through the Port Security Grant Program (PSGP) and the  
Transit Security Grant Program (TSGP)

This Information Bulletin (IB) provides guidance to Port Security Grant Program (PSGP) and Transit Security Grant Program (TSGP) grantees and sub-grantees that have received funding for the installation and operation of TWIC readers, networks, and support systems in their port area(s), facility(ies), and vessel(s).

Collaboratively, the Federal Emergency Management Agency (FEMA), the United States Coast Guard (USCG), and the Transportation Security Administration (TSA) are issuing the following interim guidance.

TSA is pilot testing TWIC systems in a number of port locations throughout the country. This pilot program is expected to be complete in early 2011. It is estimated that the Final Rule specifying the use of TWIC qualified products and equipment—primarily TWIC card readers—will not be finalized prior to Calendar Year 2012.

A number of grantees and sub-grantees have PSGP and TSGP awards for the installation of TWIC readers, networks, support systems, and other related hardware. Based on the current estimate, the Final Rule will not be published in time for grantees to purchase equipment from a TWIC Qualified Products List prior to the expiration of availability of funds in accordance with 31 USC 1552.

To ensure successful completion of these projects and timely expenditure of grant funds, the following guidance is provided:

- When contracting for card readers, require that the TWIC readers are on the TSA Initial Capability Evaluation (ICE) list. The ICE list is posted on the TWIC section of TSA's public internet site at: [http://www.tsa.gov/assets/pdf/twic\\_ice\\_list.pdf](http://www.tsa.gov/assets/pdf/twic_ice_list.pdf). The ICE list is updated each time a reader is submitted for evaluation and satisfactorily demonstrates its ability to process TWIC card information correctly. It is strongly recommended that TWIC equipment purchasers develop an agreement with vendor(s) to ensure procured equipment will be upgradeable or exchangeable to meet the Final Rule specification when published. TWIC equipment purchasers are advised to conduct a suitability analysis for their facility prior to entering into an agreement with one or more vendors. Among the things the analysis should include are:
  - Compatibility with planned or legacy physical access control system
  - Ability of fixed readers to withstand environmental conditions anticipated if installed outdoors
  - Ability to view reader screen in bright or low light conditions if installed outdoors
- If a grantee requests to re-scope an existing award, all new projects must meet maritime security risk mitigation within the port area or the facility. Projects funded by re-scoping will not be eligible for additional grant funding. The re-scoping request must include a revised budget, a revised timeline of milestones for completion, justification for the changes requested and the Captain of the Port's (COTP) determination. Re-scoping projects may take several months and will include financial and Environmental Historical Preservation (EHP) reviews. Re-scoping will be approved at the Program Analyst's discretion with consideration for time available within the grant period of performance, Captain of the Port (COTP) determination, and applicability to PSGP priorities for the Fiscal Year of the award.

If you have additional questions, please contact your FEMA GPD Program Analyst.

<b>Question#:</b>	8
<b>Topic:</b>	enrollment
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

**Question:** What is the total cost of TWIC card enrollment, to date?

**Response:** The Transportation Security Administration (TSA) views enrollment costs as the full cost to receive a TWIC, which encompasses all costs of the TWIC program. Therefore, total cost to date is \$356 million, of which \$264 million is the TSA's cost (\$103M appropriated funds; \$161M fees) and \$92 million is the private sector contractor cost.<sup>1</sup>

<sup>1</sup> TSA last received appropriated funding for TWIC in 2008. Since then, TWIC has been a fee-funded activity.

<b>Question#:</b>	9
<b>Topic:</b>	report 1
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

**Question:** GAO's May 2011 report states that the U.S. Coast Guard threat assessment states that terrorists are most likely to use vehicle bombs to strike port facilities. How does use of the TWIC card address this vulnerability?

**Response:** The genesis of the Transportation Worker Identification Credential (TWIC) was in response to threats and vulnerabilities identified in the transportation system. The TWIC is a necessary credential for transportation workers to obtain because it ensures the maritime (and surface transportation) workforce member has been vetted through the Transportation Security Administration (TSA) security threat assessment.

TWIC is part of a layered port facility security system and further ensures that only people with legitimate business can gain access to the Maritime Transportation Security Act (MTSA)-regulated port facility.

A terrorist with a Vehicle Borne Improvised Explosive Device would not be able to gain entry into a MTSA-regulated port facility if properly screened by the private security force. However, this layer of security does not eliminate an insider threat, in which one of the workers who has already received a TWIC and passed a background check, becomes a threat. Accordingly, there is a layered port facility security system, and TWIC is only one vital part of that process.

<b>Question#:</b>	10
<b>Topic:</b>	report 2
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

**Question:** GAO's May 2011 report indicates that the program's internal control deficiencies prevent the TWIC program from achieving its goals. What will it cost and how long will it take to correct all of the deficiencies and will the deficiencies be corrected prior to issuing the reader rule for the TWIC program?

**Response:** A number of weaknesses have already been addressed through low or no cost procedural changes. Other mitigation actions require regulation or rule changes to be implemented, which will require sufficient time for notice and comments. Still others require additional information before costs and timeframes can be estimated. One planned effort is the joint TSA/Federal Bureau of Investigation (FBI) "rap-back" pilot that is currently in development. As envisioned under the rap-back pilot, if any new criminal record information associated with the fingerprints of TWIC applicants previously checked arises, TSA would be notified of the criminal activity. TSA would then adjudicate the additional criminal records and determine if the TWIC should be revoked. With the possible exception of actions requiring a rule change, all internal control weaknesses should be addressed prior to the implementation of the TWIC reader rule.

<b>Question#:</b>	11
<b>Topic:</b>	GAO 1
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

**Question:** Given that GAO was able to obtain authentic TWICs using counterfeit identity documents, what is the impact of an individual obtaining an authentic TWIC through the use of counterfeit identity documents? To what extent would the use of authentic TWICs acquired using fraudulent identities defeat the presumed advantages of using TWICs with electronic card readers?

**Response:** The Transportation Worker Identification Credential (TWIC) program contains safeguards against persons enrolling using a false identity. Enrollment officers receive training in identifying counterfeit documents and use document scanners to review the security features on presented identity documents. Also, the TWIC Security Threat Assessment includes a fingerprint-based criminal history check, which should identify cases where a person has a criminal record under an identity that is different than the identity being presented at enrollment.

In addition, possession of a TWIC does not guarantee access to secure areas of the facilities. The individual facility has a responsibility to determine if access privileges should be granted based on the business case of the individual presenting the TWIC.

TWIC readers can determine whether or not the certificates on the card have been revoked via the Canceled Card List, enabling the port facility to prevent a genuine TWIC from being used if it discovers that the holders enrolled under a fraudulent identity.

The extent of using an authentic/legitimate TWIC acquired through fraudulent documents exposes the vulnerability of all credentialing security system regardless of whether TWIC readers are used.

<b>Question#:</b>	12
<b>Topic:</b>	problems
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

**Question:** TWIC holders have reported problems with the durability of their TWICs. What operational environment testing did TSA conduct on card durability? Was this testing comparable to the environmental testing that DOD conducted on its Common Access Cards (CAC)? If not, why not?

**Response:** The Transportation Worker Identification Credential (TWIC) program uses card stock approved by General Services Administration (GSA) for the biometric credentials issued to all Federal employees and contractors. It is also the same card stock used for the Common Access Credential (CAC). Because this card stock is already approved for applications within the Federal government, TSA has not conducted any further card stock testing. A very small sampling of TWIC cards were tested in a manner similar to the forensic testing routinely performed on the CAC card stock. The results were similar to those of the Department of Defense (DoD) forensic tests of the CAC. An improved process for manufacturing card stock was introduced in September 2009 and has resulted in fewer card failure issues.

<b>Question#:</b>	13
<b>Topic:</b>	profile
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

**Question:** Given the different risk profile and diversity of maritime facilities and their associated security needs, the technological challenges associated with using TWIC cards and readers, and the potential substantial costs of implementing the program, should consideration be given to implementing the program in a more risk-based manner? Are TWICs and TWIC readers needed for all maritime workers and facilities?

**Response:** The most important part of the Transportation Worker Identification Credential (TWIC) process is the Transportation Security Administration's security threat assessment conducted for the maritime (and surface transportation) workforce.

The Coast Guard agrees that there should be a risk-based approach to implementing TWIC reader requirements. The Coast Guard published an Advanced Notice of Proposed Rulemaking (ANPRM) on TWIC reader requirements on March 27, 2009, which proposed a risk-based framework for categorizing MTSA-regulated vessels and facilities into three risk groups. Based on that framework, the ANPRM proposed to require vessels and facilities in the lowest risk group to implement a robust TWIC inspection regime, but without requiring TWIC readers. The ANPRM proposed TWIC reader requirements for vessels and facilities in the higher risk groups. Currently, the Coast Guard is diligently working to evaluate all available data before publishing the TWIC Reader Notice of Proposed Rulemaking (NPRM), which will be informed by the public comments received in response to the ANPRM, as well as data from the Department of Homeland Security's TWIC reader pilot report.

<b>Question#:</b>	14
<b>Topic:</b>	VIPR
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

**Question:** According to a May, 2010 GAO report, “performance measures ha[ve] not been fully established to assess the results of VIPR deployments.” What metrics have you established to evaluate the efficiency and effectiveness of this program?

What terrorist activity have VIPR deployments averted?

**Response:** During 2010, the Visible Intermodal Prevention and Response (VIPR) program initiated four measures that are reported quarterly to senior leadership at the Transportation Security Administration (TSA) and at the Department of Homeland Security (DHS):

1. The number of operations conducted in all modes of surface transportation, which is an indicator of the extent stakeholders demonstrate their belief in the benefits of VIPR activities at their mass transit, maritime, highway infrastructure, freight rail and pipeline facilities.
2. The number of operations conducted in all modes of aviation transportation, which is an indicator of the extent stakeholders demonstrate their belief in the benefits of VIPR activities at their commercial aviation, air cargo, and general aviation facilities.
3. The percentage of stakeholders with repeat operations each quarter, under the assumption that stakeholders continue their involvement with VIPR as a result of the perceived confidence and protection benefits that are achieved.
4. The percentage of National Special Security Events (NSSE) and Special Event Assessment Rating level one and two (SEAR 1 and SEAR 2) events that VIPR assets support by deploying at transportation locations associated with these high profile and high risk events. VIPR assets augment the other assets providing protective support for the events.

Further, the VIPR program is in the process of implementing a direct stakeholder survey that will assist TSA in developing a baseline for assessing the effectiveness of deployed capabilities through the feedback received. If the current schedule is achieved, TSA anticipates this survey should be initiated in the third quarter of this fiscal year.

<b>Question#:</b>	14
<b>Topic:</b>	VIPR
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

A primary objective of VIPR is to deter and disrupt potential terrorist activity. The program can be successful at achieving both of these objectives while never knowing that terrorist actions were averted or becoming aware of only a small percentage of instances. The VIPR deployment framework uses randomness as a key operating principle to increase the level of unpredictability of a visible presence to disrupt and deter the opportunity for terrorist actions.

<b>Question#:</b>	15
<b>Topic:</b>	GAO 2
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

**Question:** In the GAO's March 2011 report on the Screening Partnership Program cost analysis, GAO concluded: "...TSA estimated that SPP airports would cost 3 percent more to operate in 2011 than airports using federal screeners." Does TSA abide by this statistical analysis? Is that 3% within the margin of error? List all of the cost factors TSA considered when conducting this cost analysis.

**Response:** The analysis GAO reviewed used two comparison points to estimate and compare costs of private screening to Federal screening for fiscal year 2011. The first Federal cost estimate assessed the impact of private screening to TSA's budget and included costs for labor, benefits, premium pay, awards, attrition, administrative staff, overhead costs, new hire costs, consumables, facilities, headquarters support, training, and uniforms. This comparison showed that private screening costs were approximately nine percent higher than estimates of Federal screening costs. The second Federal cost estimate compared the cost of privatized screening to one that included all of the items mentioned above and the full imputed retirement costs, worker's compensation, general liability insurance, and adjustments for corporate taxes. This latter method is utilized and recommended by the United States Office of Personnel Management (OPM). Using OPM's assumptions produced estimates showing that private screening during Fiscal Year 2011 would cost three percent more than federal screeners. Cost comparisons are completed annually, and TSA does not expect there to be a three percent difference each year. Currently, there is no "margin of error" associated with the Federal cost estimates, however, DHS is currently developing a confidence interval for use with estimating Federal costs in the future. This initiative will be complete in late June or early July 2012.

<b>Question#:</b>	16
<b>Topic:</b>	GAO 3
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

**Question:** In that same report GAO also indicated that the "...TSA had taken actions that partially addressed the four remaining limitations related to cost, but needs to do more to fully address them." Has TSA addressed the four remaining limitations related to cost? (Those limitations were: 1.) uncertainty in the cost estimates for non-SPP airports; 2.) failure to account for screening performance and costs associated with a particular level of performance; 3.) failure to ensure that cost data collected were reliable; and 4.) failure to document key assumptions and methods used in sufficient detail to justify the reasonableness of costs.)

**Response:** TSA has partially addressed and continues to assess how it can best address the four identified cost limitations. TSA plans to update the study with more recent data and present the information according to managerial cost accounting standards. It is unlikely that the updates will materially affect the results of the cost study per the reasons provided below.

The following provides a status update for the four remaining cost limitations:

1. Uncertainty in the cost estimates for non-Screening Partnership Program (SPP) airports:

TSA's cost methodology for comparing private screening and federal screening at the same airport results in a limited degree of uncertainty because SPP airport costs are actual, while federal costs are estimated on the basis of TSA's technical approach. However, this uncertainty is not significant. TSA federally screened airports are staffed in accordance with the TSA staffing allocation model. Although an airport may exceed its allocation or burn lower than its allocation, these variations are small and unlikely to affect cost estimates, considering the allocation is based on TSA procedures and requirements. Over the past several years, TSA has improved its cost studies to include various assumptions, such as assumptions for general liability insurance, worker's compensation and corporate tax adjustment. The studies now produce a range of estimated costs for federal screening.

2. Failure to account for screening performance and costs associated with a particular level of performance:

<b>Question#:</b>	16
<b>Topic:</b>	GAO 3
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

During discussions with the Government Accountability Office (GAO) concluding in January 2011, TSA provided GAO an analysis of how changes in assumptions affect cost estimates. During GAO's reviews, TSA provided multiple comparisons showing different assumptions and methodologies.

TSA informally attempted to determine if cost and performance were related. The results showed there is no direct relationship between private costs and performance levels. However, while TSA does account for performance bonuses in its calculation of federal costs to try to address this concern, it is difficult to estimate costs with performance as a variable. Furthermore, the Aviation and Transportation Security Act (ATSA) requires that screening performance under SPP be equal to the performance level of Federal screening. TSA evaluates performance based on that ATSA requirement. However, TSA welcomes GAO's assistance to conduct this analysis.

### 3. Failure to ensure that cost data collected were reliable:

During the fall of 2010 and winter of 2011, TSA provided to GAO with a comprehensive set of documents, data, and briefings on the information and methodologies used. TSA believes the SPP cost data used is highly reliable because it is actual budget data from the U.S. Coast Guard financial system, actual invoices from SPP contractors, actual payroll data from the National Finance Center, and actual employee information.

TSA can compile the information in GAO's preferred format with a reference guide according to managerial cost accounting procedures.

### 4. Failure to document key assumptions and methods used in sufficient detail to justify the reasonableness of costs:

TSA provided GAO documents, data, and briefings on the information and the methodologies used during the fall of 2010 and winter of 2011. Costs estimates completed following the GAO's study have incorporated more detail on the assumptions used. TSA welcomes GAO's assistance in making any further modifications.

<b>Question#:</b>	17
<b>Topic:</b>	rules
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable John L. Mica
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

**Question:** In 2003, Congress mandated that TSA issue repair station security rules. TSA still has not finalized the rules and because of the agency's inaction, since 2008, the FAA has been prohibited from certificating new foreign repair stations. Given that the repair station security rules were mandated in 2003, what is the reason for not finalizing repair station security rules in a timely manner?

**Response:** As a result of comments received from our numerous industry partners, as well as the general public on the Notice of Proposed Rulemaking (NPRM) published on February 2009, and due to requirements of Executive Order 12866, Regulatory Planning and Review (58 FR 51735, October 4, 1993) and Executive Order 13563, Improving Regulation and Regulatory Review (76 FR 3821, January 21, 2011), TSA recently completed the economic analysis and forwarded the Final Rulemaking to DHS on May 14, 2012. TSA is sensitive to the issues created by the delay in the publication of the Final Rule and is working diligently to complete this task.

<b>Question#:</b>	18
<b>Topic:</b>	medical implants
<b>Hearing:</b>	TSA Oversight Part III: Effective Security or Security Theater?
<b>Primary:</b>	The Honorable Raul Labrador
<b>Committee:</b>	OVERSIGHT & GOV RFORM (HOUSE)

**Question:** Will people with medical implants always be subjected to invasive patdowns?

What will you do to ensure that people with proven medical implants don't have to be subjected to invasive patdowns time after time?

Do you have a plan to allow for less invasive screening procedures for those who can prove that they have metal medical implants?

**Response:** TSA already uses new technology, Advanced Imaging Technology (AIT), to reduce the likelihood that individuals with medical implants will require additional pat-down screening. The vast majority of individuals with medical implants can be safely screened by AIT. If an AIT anomaly is observed, generally only the area of the anomaly requires additional screening. Individuals with metal implants may request to be screened by AIT rather than by a metal detector because they will be less likely to alarm the AIT.

TSA continues to explore other screening methods that would resolve alarms and be less intrusive to individuals with medical conditions. Currently, individuals with a medical condition, disability, or medical device may present a "Disability Notification Card" that informs a Transportation Security Officer (TSO) of the individual's medical condition. These cards are helpful in discreetly communicating information to the TSO so they can determine the best way to screen an individual with a medical device, but they do not exempt the individual from screening.

TSA has also launched TSA Cares, a helpline number designed to assist travelers with disabilities and medical conditions. Travelers may call TSA Cares toll free prior to traveling with questions about screening policies, procedures, and what to expect at the security checkpoint. TSA Cares serves as an additional, dedicated resource specifically for passengers with disabilities, medical conditions or other circumstances or their loved ones who want to prepare for the screening process prior to flying.