AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

TSA OVERSIGHT PART 2: AIRPORT PERIMETER SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, HOMELAND DEFENSE AND FOREIGN OPERATIONS

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

JULY 13, 2011

Serial No. 112–75

Printed for the use of the Committee on Oversight and Government Reform



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

U.S. GOVERNMENT PRINTING OFFICE

71–820 PDF WASHINGTON : 2012

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

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

DARRELL E. ISSA, California, *Chairman*

DAN BURTON, Indiana
JOHN L. MICA, Florida
TODD RUSSELL PLATTS, Pennsylvania
MICHAEL R. TURNER, Ohio
PATRICK T. MCHENRY, North Carolina
JIM JORDAN, Ohio
JASON CHAFFETZ, Utah
CONNIE MACK, Florida
TIM WALBERG, Michigan
JAMES LANKFORD, Oklahoma
JUSTIN AMASH, Michigan
ANN MARIE BUERKLE, New York
PAUL A. GOSAR, Arizona
RAÚL R. LABRADOR, Idaho
PATRICK MEEHAN, Pennsylvania
SCOTT DESJARLAIS, Tennessee
JOE WALSH, Illinois
TREY GOWDY, South Carolina
DENNIS A. ROSS, Florida
FRANK C. GUINTA, New Hampshire
BLAKE FARENTHOLD, Texas
MIKE KELLY, Pennsylvania

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. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MIKE QUIGLEY, Illinois
DANNY K. DAVIS, Illinois
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont
JOHN A. YARMUTH, Kentucky
CHRISTOPHER S. MURPHY, Connecticut
JACKIE SPEIER, California

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*

SUBCOMMITTEE ON NATIONAL SECURITY, HOMELAND DEFENSE AND FOREIGN OPERATIONS

JASON CHAFFETZ, Utah, *Chairman*

RAÚL R. LABRADOR, Idaho, *Vice Chairman*
DAN BURTON, Indiana
JOHN L. MICA, Florida
TODD RUSSELL PLATTS, Pennsylvania
MICHAEL R. TURNER, Ohio
PAUL A. GOSAR, Arizona
BLAKE FARENTHOLD, Texas

JOHN F. TIERNEY, Massachusetts, *Ranking Minority Member*
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont
JOHN A. YARMUTH, Kentucky
STEPHEN F. LYNCH, Massachusetts
MIKE QUIGLEY, Illinois

CONTENTS

	Page
Hearing held on July 13, 2011	1
Statement of:	
Sammon, John, Assistant Administrator, U.S. Transportation Security Administration; Stephen M. Lord, Director, Homeland Security and Justice Issues, U.S. Government Accountability Office; TJ "Jerry" Orr, airport director and operator, Charlotte International Airport; Rafi Ron, president, New Age Security Issues, former director of security Tel Aviv-Ben Gurion International Airport; and William Parker, inspector, K–9 Unit, Amtrak Police Department	9
Lord, Stephen M.	13
Orr, TJ "Jerry"	33
Parker, William	46
Ron, Rafi	41
Sammon, John	9
Letters, statements, etc., submitted for the record by:	
Lord, Stephen M., Director, Homeland Security and Justice Issues, U.S. Government Accountability Office, prepared statement of	15
Orr, TJ "Jerry", airport director and operator, Charlotte International Airport, prepared statement of	35
Parker, William, inspector, K–9 Unit, Amtrak Police Department, prepared statement of	48
Ron, Rafi, president, New Age Security Issues, former director of security Tel Aviv-Ben Gurion International Airport, prepared statement of	42
Sammon, John, Assistant Administrator, U.S. Transportation Security Administration, prepared statement of	11
Tierney, Hon. John F., a Representative in Congress from the State of Massachusetts, prepared statement of	5

TSA OVERSIGHT PART 2: AIRPORT PERIMETER SECURITY

WEDNESDAY, JULY 13, 2011

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY, HOMELAND DEFENSE AND FOREIGN OPERATIONS,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:30 a.m., in room 2154, Rayburn House Office Building, Hon. Jason Chaffetz (chairman of the subcommittee) presiding.

Present: Representatives Chaffetz, Mica, Platts, Gosar, Farenthold, Tierney, and Lynch.

Staff present: Thomas A. Alexander, senior counsel; Kate Dunbar, staff assistant; Linda Good, chief clerk; Christopher Hixon, deputy chief counsel, oversight; Mitchell S. Kominsky, counsel; Justin LoFranco, deputy director of digital strategy; Laura L. Rush, deputy chief clerk; Sang Yi, professional staff member; Jaron Bourke, minority director of administration; Kevin Corbin, minority staff assistant; and Carlos Uriarte, minority counsel.

Mr. CHAFFETZ. Good morning. The committee will come to order. We appreciate you all being here for this oversight hearing, part number 2, regarding the TSA airport perimeter screening. I'd like to welcome Ranking Member Tierney and members of the subcommittee and members of the audience who are here and participating with us, and those of you that are watching on television.

Today's proceedings are the second in a series of hearings designed to evaluate the status of U.S. airport security and the policies employed by the Department of Homeland Security. There are a number of concerns that have been highlighted to be drawn out here today. First and foremost, we have learned that there have been 25,000 security breaches at U.S. airports since November 2001. And I do appreciate the TSA in tracking and providing that data, but obviously those are the ones that we know about, and the deep concern is what about the ones that we don't know about, and the creativity and things that can happen in the future.

We also are deeply concerned about the TSA failing to conduct threat vulnerability assessments in order to identify gaps in perimeter screening. In 2009 the GAO had concluded there were 87 percent of these airports that had not had these threat assessments done, and that number really has not changed.

TSA also lacks a national strategy to secure commercial airports and access control; this, again, coming from a GAO report that says

that the Nation's 457 commercial airports have not, "been guided by a unifying national strategy."

Also concerned about more than 900,000 security badges at these 457 airports, and the dangers that that can lead to and the challenges that that presents.

We're also concerned about what's happening at some of our Nation's airports; for instance, at JFK the investigative reports show that at least "a quarter mile of the perimeter fence is down, leaving a gaping hole in security along a main JFK runway." This project is 4 years behind schedule.

Also concerned about what happened at Dallas Love Field. The fence has been breached or damaged almost 20 times in less than 5 years. In fact, air traffic control tapes show that pilots on the ground were unsure of what to do when a pickup truck crashed through a fence and drove onto the tarmac on August 19, 2010. One of the pilots inquired, "Tower, what's the protocol for something like this? If he's coming at us, can we move?" Airport control tower responded, "Just hold position."

We are also concerned about what's happening at LAX. They have 8 miles of fence there, built in stages over the past decade, and yet no one consistent standard has happened. We have spent nearly—we will have spent nearly $500 million on AIT machines—I call them the whole body imaging machine—by the time we get to the year 2013. And yet these machines, there are parts and gaps in that security that don't work.

I happen to believe that there's a better, smarter way to do this that is more secure, less invasive, and we're going to hear some testimony today talking about the canine units and what they are able to do. And I look forward to hearing that testimony.

We're also concerned that these AIT machines, or whole body imaging machines, would not have found some of the weapons that were attempted to be used in the December 2009 incident. And the list goes on.

TSA has spent millions and millions of dollars in technology that has not worked. You remember the 207 puffer machines. After spending $30 million and having those deployed, those were put back on the shelf.

The challenge before us is great. It's immense. It's real. And we have to deal with that threat to our Nation. It's not going to go away. There is no end to the creativity of terrorists. And while I have heard the press recount say that well, let's remember the 25,000 security breaches are 1 percent, or even less than, 1 percent, unfortunately, we have to be right all the time. Terrorists only have to get lucky once.

A lot of what we have been participating here, in my personal opinion, has been security theater, and has not truly done the job to secure the airports to the degree that we need to. And I think one of the personal challenges that we have as a Nation is how do we become more secure and yet less invasive; that we don't give up every personal liberty in the name of security. And we have to find that proper balance. It's a difficult one, knowing that the threat is real.

So I look forward to this hearing today. We are going to also—so rather than wax on, I'd love to hear from the panel. But at this

time I'd like to recognize the ranking member of this subcommittee, the gentleman from Massachusetts, Mr. Tierney, for his opening statement.

Mr. TIERNEY. Thank you, Mr. Chairman. And thank our witnesses for being here this morning as well.

Look, we understand that we are going to address some important issues here today. And one of them, for instance, is the Screening Passenger Observation Techniques [SPOT] program. Our Government Accountability Office has criticized that SPOT program, saying that it lacks appropriate scientific validation.

The Department of Homeland Security has released a study that it says showed SPOT is more effective than random screening, but it does acknowledge that it didn't address whether behavioral analysis is actually an effective way to detect potential terrorists. Now, they've spent $750 million on it already; they're asking for another $250 million. I think it's pretty critical that we, with that significant investment out there, that we take a good look and scrutinize whether or not this program actually is effective at identifying potential threats to security.

We're also going to discuss the screening of checked baggage using the explosive detection technology. Congress mandated 100 percent screening of checked bags by the Transportation Security Agency, but it's been slow to implement those standards at airports across the country,

Again, the Government Accountability Office said that despite the regulations being in effect in 2005, the expositive detection technology requirements weren't put in place till 2009.

Turning to the issue of perimeter security, there have been some high-profile breaches that we are all aware of. Specifically, we will hear today about the tragic incident that occurred just outside of Boston's Logan Airport, where a young man fell from a plane as it approached the airport for landing. According to news reports, he likely gained access to the plane after breaching airport perimeter security in Charlotte. This is not a unique incident, unfortunately.

We have also heard about serial security breaches by Mr. Ronald Wong, who was somehow able to make it on to a plane leaving JFK Airport in New York to San Francisco with a stolen boarding pass.

The Government Accountability Office has also raised concerns about perimeter security at our Nation's airports. In 2009 they found the TSA had failed to implement a national strategy to address perimeter security, and that only a small percentage of airports had completed joint vulnerability assessments. This, again, raised serious questions that have to be addressed.

So as we evaluate these incidents and the challenges, it's probably important for us to take the time to understand what security functions the Transportation Security Administration is not directly responsible for. And one of those is the perimeter area. They are not principally responsible for perimeter security at airports. That perimeter security is primarily the responsibility of airport operators, while TSA's role is to ensure that the operator is adhering to an appropriate security plan that meets Federal standards.

So, as I said at the last hearing on TSA, the Agency has a difficult and unenviable task, but it's our responsibility, our role, to provide constructive criticism with which you at TSA can strike the

balance between security, convenience and cost, hopefully, weighing heavily on the security aspect. I hope our hearing today can help TSA do just that. And I thank the chairman again for bringing us together.

Mr. CHAFFETZ. Thank you.

[The prepared statement of Hon. John F. Tierney follows:]

Opening Statement
Rep. John Tierney, Ranking Member

Subcommittee on National Security, Foreign Operations and Homeland Defense
Hearing on "TSA Oversight Part 2 - Airport Perimeter Security"

July 13, 2011

Thank you, Chairman Chaffetz, for convening this hearing today. And thank you to our witnesses for agreeing to testify.

Today's hearing will address the important issue of airport security and airport perimeter security. One TSA program that has been the target of much scrutiny is the Screening Passenger Observation Techniques or SPOT program. GAO has criticized the SPOT program as lacking appropriate scientific validation. DHS has since released a study that it says shows SPOT is more effective than random screening, but they have admitted the study did not address whether behavioral analysis is actually an effective way to detect potential terrorists. As GAO noted, DHS has invested over $750 million in SPOT since 2007 and has requested an additional $250 million for fiscal year 2012. Given this significant investment, I think it is important to understand whether the program is actually effective at identifying potential threats to aviation security.

We will also discuss the screening of checked baggage using Explosive Detection Technology. Since Congress mandated 100 percent screening of checked baggage by TSA, the agency has been slow to implement new standards at airports across the country. In fact, GAO found that TSA did not begin deploying the 2005 Expositive Detection Technology requirements until 2009, fully four years after the standards were released.

Turning to the issue of perimeter security, there have been some high profile breaches that should give us cause for concern. Specifically, we will hear today about a tragic incident that occurred just outside Boston's Logan airport where a young man fell from a plane as it approached the airport for landing. According to news reports, he likely gained access to the plane after breaching airport perimeter security in Charlotte. This is not a unique incident. We've also heard about serial security breaches by a Mr. Ronald Wong, who was somehow able to make it onto a plane leaving JFK airport in New York for San Francisco with a stolen boarding pass.

GAO has also raised concerns about perimeter security at our nation's airports. In 2009, they found that TSA had failed to implement a national strategy to address perimeter security, and that only a small percentage of airports had completed joint vulnerability assessments. Again, this raises serious questions that must be addressed.

As we evaluate these incidents and challenges, it is important for us to take the time to understand what security functions TSA is and is not directly responsible for at our nation's airports. I know we are all familiar with TSA's lead role in screening passengers and baggage.

Because the central focus of this hearing is perimeter security, it is important to note that TSA is *not* principally responsible for perimeter airport security. Perimeter security is the primary responsibility of the airport operator while TSA's role is to ensure that the operator is adhering to an appropriate security plan that meets Federal standards.

As I said at the last hearing on TSA, the agency has a difficult and unenviable task. Our role is to provide constructive criticism with which TSA can strike the right balance of security, convenience and cost. I hope our hearing today can help TSA do just that.

Mr. CHAFFETZ. We will now recognize the chairman of the Transportation Committee, and also a member of this subcommittee, the gentleman from Florida, Mr. Mica, for his opening statement.

Mr. MICA. Well, thank you, Mr. Chairman. And thank you, Mr. Tierney, for your leadership and also pursuing very important issues relating to transportation security and holding a very important Agency accountable.

Having been involved with the TSA and actually picked the name for the Agency and helped craft its enabling legislation some 10 years ago, I've had a chance to monitor its activities closely. And unfortunately, I become more and more concerned with the billions of dollars that are being expended. Some of it just astounds me. We've created an Agency that's actually run pell mell away from security and turned into a huge, unthinking, nonrisk-based bureaucracy. Everywhere I turn, I'm appalled at what's taking place.

Recently I had the opportunity to go to our State Capitol, Tallahassee, and I left the airport to pick up a rental car. And the airport is located on about a 16-foot embankment that actually is an embankment across the entire length of the airport. Here's the front of the airport. Here's the embankment, 16 feet high. And just to show you—we're talking about airport security and perimeters—how idiotic we could be in implementation of any requirement like this. But this is the parking space for rental cars. This is a 16-foot embankment. You can see up here where cars go through the entrance of the airport.

Now, there's a new airport administrator. He wasn't familiar with all of the details, but we're going to do a thorough investigation of this. This is just one instance, again, of a nonthinking Agency.

I don't know of any explosive device that could possibly penetrate 16 feet here, except maybe a nuclear weapon. I don't know how much it cost to put these barriers here, but again, forcing a small airport—or if TSA paid for an idiotic expense, not to mention the cost to the taxpayer or the airport. But then, of course, they would never consider the economic loss to the car rental firm or to the revenue of the airport.

But every time, everywhere I turn, I see a disregard for the taxpayer. This is just one instance and one small community. Again, just an unthinking Agency. Their budget is, what, in the $8 billion range?

Then I open the paper a week or two ago when I returned to Washington, and I look at this ad. Now, of course, the Humane Society is looking for a vice president of Federal Affairs and they have a little—I'd say it's about a sixth of the page. But we have a four-color, half-page ad for a Deputy Assistant Administrator for Legislative Affairs in this and other Capitol Hill publications. Half page. Only total disregard for taxpayers' resources could you expend money on—whether it's a venture like this at my State Capitol airport, or in a Capitol Hill publication. And I'm going to request, too, an accounting for expenditure of this money.

And let me just tell TSA, too, that if you refuse to cooperate with my committee, the Transportation and Infrastructure Committee, I have had and will continue to have the cooperation of both this subcommittee on which I serve, and the full committee. Mr. Issa

and the chairman here have agreed to cooperate to get this information. And we will get the data, whether it's this or other activities such as you've refused to provide information to us on regarding your expenditure of your national deployment force where you can't hire people, or people leave their jobs and you have to fly them in, put them up at hotels, pay their expenses, and pay them a per diem. Whether it's that issue or more than a dozen pending items, we will get the information. We will investigate. We will protect the taxpayers who are paying the bulk of the expenses for this fiasco.

So thank you for holding this hearing. We'll get to some issues and questions in a few minutes. And I yield back.

Mr. CHAFFETZ. Thank you. We'll now recognize the gentleman from Massachusetts, Mr. Lynch, if he'd like an opening statement. We will recognize you for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman. Very briefly, obviously the interest of airport perimeter security is a tremendous one for all of us. I know that we have spent enormously on the safety and security of the processes within our airports. But this is something that—the security of our perimeters of these airports has become much more of a concern since the fairly recent incidents that involved my district. The young man who was apparently stowed away on an aircraft recently from, I believe it was South Carolina, to Logan Airport in Boston, actually was found deceased in my district, in the town of Milton in my district. So I was able to see up close the tremendous concern generated by this, the hardship on the family, the concerns of all the law enforcement involved as well, and obviously the concern within the aviation community.

So I think it is worthwhile to spend some time to redouble our efforts to focus our resources on an area that we believe has been neglected.

And I want to thank the witnesses here for their willingness to come before us to help us with this task, to help the committee to make sure that we're being thorough in our examination, that we're not overlooking anything, and that, you know, as a result of this incident and some others, that at the end of this process the American flying public will be safer and our communities will be safer, and our airports will be more secure. That's the goal here for both Democrats and Republicans. That's our intent here.

And again, I want to thank the witnesses for coming before this committee to help us with our work. I yield back.

Mr. CHAFFETZ. Thank you.

I'd like to now introduce our panel so they can be prepared for their opening statements.

Mr. John Sammon is the Assistant Administrator with the Transportation Security Administration. We do appreciate your being here.

Mr. Stephen Lord is the Director of the Homeland Security Team at the Government Accountability Office.

Mr. Jerry Orr is the aviation director at the Charlotte Douglas International Airport.

Mr. Rafi Ron is the president of New Age Security Solutions, and is the former director of security at Tel Aviv-Ben Gurion International Airport.

And Inspector William Parker is the commander of Amtrak Police Department's K–9 Unit. We appreciate you being here as well.

Pursuant to committee rules, all witnesses will be sworn in before they testify. Please rise, if you would, and raise your right hands.

[Witnesses sworn.]

Mr. CHAFFETZ. Thank you. Please be seated. Let the record reflect that all witnesses answered in the affirmative.

In order to allow time for discussion, we would appreciate if you'd limit your verbal testimony to 5 minutes or less. Your entire written statement will be entered into the record.

So with that, we'll start with Mr. Sammon. You're recognized for 5 minutes.

STATEMENTS OF JOHN SAMMON, ASSISTANT ADMINISTRATOR, U.S. TRANSPORTATION SECURITY ADMINISTRATION; STEPHEN M. LORD, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; TJ "JERRY" ORR, AIRPORT DIRECTOR AND OPERATOR, CHARLOTTE INTERNATIONAL AIRPORT; RAFI RON, PRESIDENT, NEW AGE SECURITY ISSUES, FORMER DIRECTOR OF SECURITY TEL AVIV-BEN GURION INTERNATIONAL AIRPORT; AND WILLIAM PARKER, INSPECTOR, K–9 UNIT, AMTRAK POLICE DEPARTMENT

STATEMENT OF JOHN SAMMON

Mr. SAMMON. Good morning, Chairman Chaffetz, Ranking Member Tierney, and distinguished members of the subcommittee. I appreciate the opportunity to appear before you today to discuss the Transportation Security Administration's responsibility regarding perimeter security at U.S. commercial airports.

I would like to emphasize three points. First, every airport has an individualized security plan of which security—perimeter security is an important piece. Two, airport authorities are responsible for executing the plan. Three, TSA is responsible for approving the plan and inspecting airport compliance with the plan.

Unlike checkpoint security, airport authority people investments play the lead role in carrying out airport perimeter security. TSA conducts airport inspections to enhance security and mitigate risk associated with perimeter integrity, including joint vulnerability assessments, special emphasis inspections, and the testing of access control processes at airports. TSA analyzes the results of these inspections and assessments to develop mitigation strategies that enhance an airport's security posture and to determine if any changes are required.

Perimeter-related airport compliance has been inspected 27,031 times over the past 16 months. Every commercial airport receives an annual security assessment, to include an assessment of perimeter and access controls. Earlier this year, TSA's Office of Security Operations initiated a special emphasis assessment and special inspection of all airports evaluating perimeter security, including fencing, non-fence manmade barriers, natural barriers, closed circuit television, electronic intrusion and motion detection devices. Assessments are complete for the largest airports, with the smaller

airports expected to be complete by September 30, 2011. The results of the inspection were collaborative improvements and also violations which may result in civil penalties.

Going beyond compliance, we work collaboratively with airport operators and airport associations, and in that collaboration, TSA issued updated and improved security guidelines for airport design and construction, as well as an innovative measures report which highlights best practices from airports of all sizes across the United States. The innovative measures report effort was the first of its kind in working closely with airports across the Nation on base lining and best practices in airport perimeter, access control, terminal frontages, and other key areas.

Over 700 measures and practices from over 100 airports were assessed as part of this groundbreaking initiative. Because of that effort, airports now have a self-assessment module and a resource allocation tool. The tool incorporates attack scenarios, vulnerability scores, consequence scores, and countermeasure success probabilities. It allows airports to baseline their security programs against other airports' innovative measures that will directly inform decisions about improvements to provide the greatest risk reduction for their money at their location.

TSA's goal is to work with airport authorities to stay ahead of evolving terrorist threats, while protecting passengers' privacy and facilitating the efficient flow of travelers and legitimate commerce. TSA's airport perimeter security initiatives are one part of that comprehensive effort.

I want to thank the committee for the opportunity to discuss this important issue. I'm pleased to answer any questions you may have.

Mr. CHAFFETZ. Thank you.

[The prepared statement of Mr. Sammon follows:]

Statement of John Sammon
Assistant Administrator, Transportation Security Administration
U.S. Department of Homeland Security before the United States House of Representatives
Committee on Oversight and Government Reform
Subcommittee on National Security, Homeland Defense, and Foreign Operations
July 13, 2011

Good morning, Chairman Chaffetz, Ranking Member Tierney and distinguished Members of the Subcommittee. I appreciate the opportunity to appear before you today to discuss the Transportation Security Administration's (TSA) mandate and responsibility regarding perimeter security at U.S. commercial airports.

As you know, the Aviation and Transportation Security Act (ATSA) (Pub.L. 107-71), enacted on November 19, 2001, authorized TSA to work with U.S. airport operators to strengthen security at access and critical control points at Federalized airports in the United States to ensure the security of passengers and aircraft. While TSA's aviation security standards, established through regulations and security directives, provide a foundation for a comprehensive national aviation security program, the unique footprint, location and requirements of each airport require each facility to have its own airport security program (ASP). Each ASP incorporates specific security elements including perimeter security measures, addressing the prevention and detection of the unauthorized entry, presence and movement of individuals and vehicles into and within secured areas and Airport Operations Areas (AOA).

In addition to ASPs, federal and local partnerships are key to screening and inspecting individuals, goods, property, vehicles and other equipment before they enter a secured area or AOA. These partnerships are critical for reducing security vulnerabilities while strengthening our resilience against terrorist attacks. TSA also conducts ongoing and comprehensive airport inspections to enhance security and mitigate risk associated with perimeter integrity, including Joint Vulnerability Assessments, Special Emphasis Inspections, and the testing of access control processes at airports. TSA analyzes the results of these inspections and assessments to develop mitigation strategies that enhance an airport's security posture, and to determine if any changes are required. TSA also works in collaboration with airport operators to identify effective practices across the industry regarding access control and perimeter security.

Preventing Terrorism and Enhancing Security
TSA secures our Nation's commercial airports through a variety of programs. The programs most familiar to the traveling public include passenger screening operations conducted by Transportation Security Officers (TSO) at security checkpoints; cargo screening; and the Secure Flight program, which fulfills a key 9/11 Commission recommendation to implement a uniform watch list matching program for all passengers traveling from, within, or bound for the U.S. against names on government terrorist watch lists.

While these are the most visible or recognized layers of security at our Nation's airports, there are other layers, less obvious to the traveling public, that play an equally important role in safeguarding our Nation against terrorist threats. These additional layers include focusing on preventing and detecting the unauthorized entry, presence and movement of individuals and ground vehicles into, and within, the secured and AOAs of an airport. TSA's risk-based and intelligence-driven Security Playbook program strengthens the transportation security environment by increasing unpredictability and providing additional layers of security. This program employs security measures at direct access points and airport perimeters and uses a variety of resources and equipment to conduct screening of individuals and vehicles entering the AOA.

Examples of the security measures that may be employed at direct access points and airport perimeters include: vehicles inspections, explosive trace detection (EDT) of individuals and property, enhanced screening, accessible property searches, and ID/media verifications, as well as behavior detection.

TSA's Role in Perimeter Security
As set forth by statute, TSA prescribes regulations for screening or inspecting individuals, goods, property, vehicles and other equipment before entry into the secured area of an airport.

Security access regulations, directives, and procedures safeguard against unauthorized persons having access to aircraft, thereby reducing opportunities for criminal violence, sabotage or other such acts. These safeguards help to ensure the safety and integrity of individuals involved in the aviation domain, including aircraft service providers and those workers involved in catering and passenger amenities onboard aircraft. Similarly, TSA requires security access programs for vendors with direct access to airfields and aircraft.

Perimeter Security is a Shared Responsibility
Unlike checkpoint security, which is carried out exclusively by TSOs, perimeter security for airports' secured areas is a mutual responsibility shared among federal, state, and local government personnel. TSA also depends upon law enforcement personnel and resources provided by the airport authority, state or local government or airport personnel to play a lead role in carrying out perimeter security responsibilities.

TSA works in consultation with airport operators and local law enforcement authorities to deploy personnel to secured areas of an airport, as needed, to counter the risk of criminal violence, air piracy, a risk to air carrier operations, or to address national security concerns.

TSIs and RSIs Conduct Assessments, Test Compliance
To counter the potential risks to perimeter security, TSA deploys Transportation Security Inspectors (TSI) to determine whether airport operators are complying with all aspects of TSA regulations and the airport's ASP, as well as to provide strategic oversight regarding an airport's compliance status. The collaborative effort between TSA and the airport results in security enhancements to the airport and, where appropriate, amendments to the airport's ASP.

TSIs conduct comprehensive airport and air carrier assessments, test for compliance regarding access control and perimeter integrity requirements, and conduct surveillance regarding a variety of security processes. When necessary, they can impose civil penalties where repeated or egregious instances of noncompliance with regulations and security procedures are found.

Just as TSOs focus their efforts toward securing a specific physical location, such as a security checkpoint, TSIs focus their assessments on security throughout the airport environments, ranging from the curbside of the airport to the outermost perimeter fence along the edge of the airport property. Regional Security Inspectors (RSIs) located at TSA headquarters also conduct annual and periodic oversight assessments of inspection activity for air carrier and airport facilities at Category X, I, and II airports.

Special Emphasis Assessment and Inspection
Earlier this year, TSA's Office of Security Operations-Compliance Programs initiated a Special Emphasis Assessment (SEA) and a Special Emphasis Inspection (SEI) of all Category X and Category I through IV airports, evaluating perimeter security, including fencing, non-fenced man-made barriers, natural barriers, closed-circuit television, electronic intrusion and motion detection devices, and other barriers. Assessments are complete for all Category X and I airports, with remaining airports expected by September 30, 2011.

Conclusion
TSA's goal at all times is to maximize transportation security and stay ahead of evolving terrorist threats while protecting passengers' privacy, and facilitating the efficient flow of travelers and legitimate commerce. TSA's airport perimeter security initiatives are one part of that comprehensive effort. I want to thank the Subcommittee for the opportunity to discuss this important issue with you today and I am pleased to answer any questions you might have.

Mr. CHAFFETZ. We'll now recognize Mr. Lord, who's from the Government Accountability Office. We'll recognize you for 5 minutes.

STATEMENT OF STEPHEN M. LORD

Mr. LORD. Thank you, Mr. Chairman, Ranking Member Tierney and members of the subcommittee. Thanks for inviting me here today to discuss aviation security issues.

The attempted 2009 Christmas Day attack provides a vivid reminder civil aviation remains an attractive terrorist target and underscores the importance of today's hearing.

Securing commercial aviation operations is difficult, given the hundreds of airports, thousands of daily flights, with millions of passengers and pieces of checked baggage. But TSA spends several billion dollars each year to help secure the system. However, risks to the system remain.

Today I'd like to discuss three layers of the system. First, TSA's behavior detection program, also called SPOT; airport perimeter and access controls; and finally, TSA's checked baggage screening system.

First, regarding TSA's behavior detection program, DHS has taken actions to validate the underlying signs of the program, but based on our past reporting more actions are needed. As we reported in May 2010, TSA deployed this program on a nationwide basis without first demonstrating that it was based on valid science. According to TSA, SPOT was deployed before a validation was completed to help address potential threats such as those posed by suicide bombers.

The good news is DHS completed an initial validation study earlier this year and found that the program was more effective than random screening in identifying so-called high-risk passengers. However, as noted in the study, the assessment was just the first step. Additional research is needed, is going to be needed to fully validate the program. And some of the recommendations made in the latest DHS study mirror those we made in our May 2010 report.

In sum, it's still an open question whether behavior detection principles could be successfully applied on a large scale for counterterrorism purposes in an airport environment.

I would now like to discuss some of the key findings from our 2009 report on airport perimeter security. In terms of progress, we noted various steps TSA had made, including implementing the random worker screening program, expanding requirements for name-based background checks, and developing new biometric security standards. However, we found that TSA had not at the time completed a comprehensive risk assessment as called for by DHS. TSA subsequently completed such an assessment in July 2010; however, the updated assessment did not include an assessment of the so-called insider threat which TSA views as a significant threat. The risks posed by insider threats will be included in the next update due later this year.

We also recommended that TSA consider making greater use of joint vulnerability assessments. These are a key tool in the TSA tool box and are completed in conjunction with the FBI. The latest

data show TSA has completed joint vulnerability assessments on about 17 percent of TSA-supervised airports, leaving about 83 percent of these airports unassessed.

The last point I'd like to discuss is TSA's efforts to deploy checked baggage screening equipment. This program is one of the largest acquisition programs within DHS. As highlighted in the report released to Representative Mica yesterday, TSA has upgraded the explosive detection requirements for this equipment but faces challenges in meeting these requirements.

The explosive detection requirements for checked baggage machines were established in 1998, and subsequently revised in 2005 and 2010 to better address current threats. However, TSA's current checked baggage screening systems do not meet the 2010 requirements. Some of the machines are operating at the levels established in 2005. The remainder are operating at levels established in 1998.

Our report describes some of the challenges TSA faces in procuring and deploying this very complicated technology. For example, DHS and TSA encounter challenges safely collecting data on the explosives physical and chemical properties. Our report contains six recommendations for improving TSA's process for acquiring these sophisticated systems. The good news is that TSA has agreed to take action to implement all six of these recommendations.

Mr. Chairman, other distinguished members of the committee, this concludes my statement. I look forward to answering your questions. Thank you.

Mr. CHAFFETZ. Thank you.

[The prepared statement of Mr. Lord follows:]

United States Government Accountability Office

GAO

Testimony
Before the Subcommittee on National Security, Homeland Defense, and Foreign Operations, Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 9:30 a.m. EDT
Wednesday, July 13, 2011

AVIATION SECURITY

TSA Has Taken Actions to Improve Security, but Additional Efforts Remain

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



GAO
Accountability * Integrity * Reliability

Highlights

Highlights of GAO-11-807T, a testimony before the Subcommittee on National Security, Homeland Defense, and Foreign Operations, Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

The attempted bombing of Northwest flight 253 in December 2009 underscores the need for effective aviation security programs. Aviation security remains a daunting challenge with hundreds of airports, thousands of aircraft, and thousands of flights daily carrying millions of passengers and pieces of checked baggage. The Department of Homeland Security's (DHS) Transportation Security Administration (TSA) has spent billions of dollars and implemented a wide range of aviation security initiatives. Three key layers of aviation security are (1) TSA's Screening of Passengers by Observation Techniques (SPOT) program designed to identify persons who may pose a security risk; (2) airport perimeter and access controls security; and (3) checked baggage screening systems. This testimony provides information on the extent to which TSA has taken actions to validate the scientific basis of SPOT, strengthen airport perimeter security and access controls, and deploy more effective checked baggage screening systems. This statement is based on prior reports GAO issued from September 2009 through July 2011 and selected updates in June and July 2011. GAO analyzed documents on TSA's progress in strengthening aviation security, among other things.

What GAO Recommends

GAO has made recommendations in prior work to strengthen TSA's SPOT program, airport security efforts, checked baggage screening efforts. DHS and TSA generally concurred with the recommendations and have actions under way to address them.

View GAO-11-807T or key components. For more information, contact Stephen M. Lord at (202) 512-8777 or lords@gao.gov.

July 13, 2011

AVIATION SECURITY

TSA Has Taken Actions to Improve Security, but Additional Efforts Remain

What GAO Found

DHS has completed an initial study to validate the scientific basis of the SPOT program; however, additional work remains to fully validate the program. GAO reported in May 2010 that TSA deployed this program, which uses behavior observation and analysis techniques to identify potentially high-risk passengers, before 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. TSA officials said that SPOT was deployed in response to potential threats, such as suicide bombers, and was based on scientific research available at the time. GAO recommended in May 2010 that DHS, as part of its study, assess the methodology to help ensure the validity of the SPOT program. DHS concurred and its April 2011 validation study found that SPOT was more effective than random screening to varying degrees. For example, the study found that SPOT was more effective than random screening at identifying individuals who possessed fraudulent documents and individuals who were subsequently arrested. However, DHS's study 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. The study noted that additional work is needed to comprehensively validate the program. TSA officials are assessing the actions needed to address the study's recommendations.

In September 2009, GAO reported that since 2004 TSA has taken actions to strengthen airport perimeter and access controls security by, among other things, deploying a random worker screening program; however, TSA has not conducted a comprehensive risk assessment or developed a national strategy. Specifically, TSA had not conducted vulnerability assessments for 87 percent of the approximately 450 U.S. airports regulated by TSA at that time. GAO recommended that TSA develop (1) a comprehensive risk assessment and evaluate the need to assess airport vulnerabilities nationwide and (2) a national strategy to guide efforts to strengthen airport security. DHS concurred and said TSA is developing the assessment and strategy, but has not yet evaluated the need to assess airport vulnerabilities nationwide.

GAO reported in July 2011 that TSA revised explosives detection requirements for its explosives detection systems (EDS) used to screen checked baggage in January 2010, but faces challenges in deploying EDS that meet these requirements. Deploying systems that meet the 2010 EDS requirements could be difficult given that TSA did not begin deployment of systems meeting the previous 2005 requirements until 2009. As of January 2011 some of the EDS in TSA's fleet detect explosives at the level established in 2005 while the remaining EDS detect explosives at levels established in 1998. Further, TSA does not have a plan to deploy and operate systems to meet the current requirements and has faced challenges in procuring the first 260 systems to meet these requirements. GAO recommended that TSA, among other things, develop a plan to ensure that EDS are operated at the levels in established requirements. DHS agreed and has outlined actions to do so.

Chairman Chaffetz, Ranking Member Tierney, and Members of the Subcommittee:

I appreciate the opportunity to participate in today's hearing to discuss three key layers of aviation security: (1) the Transportation Security Administration's (TSA) behavior-based passenger screening program, (2) airport perimeter and access controls security, and (3) airport checked baggage screening systems.[1] 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. According to the President's *National Counterterrorism Strategy* released in June 2011, aviation security and screening is an essential tool in our ability to detect, disrupt, and defeat plots to attack the homeland.[2]

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. In the almost 10 years that have passed since TSA assumed responsibility for aviation security, TSA has spent billions of dollars and implemented a wide range of initiatives to strengthen the layers of aviation security. However, risks to the aviation system remain.

In addition, while airport operators, not TSA, generally retain direct day-to-day operational responsibility for airport perimeter security and implementing access controls for secure areas of their airports, TSA has responsibility for establishing and implementing measures to improve security in these areas.[3] Criminal incidents involving airport workers using their access privileges to smuggle weapons and drugs into secure areas

[1]TSA's behavior-based passenger screening program is known as the Screening of Passengers by Observation Techniques (SPOT) program.

[2]*National Strategy for Counterterrorism*, (Washington, D.C.: June 28, 2011).

[3]For the purposes of this testimony "secure area" is used generally to refer to areas specified in an airport security program for which access is restricted, including the security identification display areas (SIDA), the air operations areas (AOA), and the sterile areas. While security measures governing access to such areas may vary, in general a SIDA is an area in which appropriate identification must be worn, an AOA is an area providing access to aircraft movement and parking areas, and a sterile area provides passengers access to boarding aircraft and where access is generally controlled by TSA or a private screening entity under TSA oversight. See 49 C.F.R. § 1540.5.

and onto planes have heightened concerns about the risks posed by workers and the security of airport perimeters and access to secure areas.

My statement today discusses the extent to which TSA has taken actions to (1) validate the scientific basis of its behavior-based passenger screening program (referred to as SPOT), (2) strengthen the security of airport perimeters and access controls, and (3) deploy more effective checked baggage screening systems.

This statement is based on our prior work issued from September 2009 through July 2011, and includes selected updates conducted from June 2011 through July 2011 on TSA's efforts to implement our prior recommendations regarding aviation security, including those related to SPOT and airport perimeters and access to secure areas of airports.[4] For our May 2010 report on SPOT, we reviewed relevant literature on behavior analysis by subject matter experts.[5] We conducted field site visits to 15 TSA-regulated airports with SPOT to observe operations and meet with key program personnel.[6] We also interviewed recognized experts in the field, as well as cognizant officials from other U.S. government agencies that utilize behavior analysis in their work. For the updates, we analyzed documentation from TSA on the actions it has taken to implement the recommendations from our May 2010 report,

[4]See GAO, *Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls*, GAO-09-399 (Washington, D.C.: Sept. 30, 2009); 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); and GAO, *Aviation Security: TSA Has Enhanced Its Explosives Detection Requirements for Checked Baggage, but Additional Screening Actions Are Needed*, GAO-11-740 (Washington, D.C.: July 11, 2011).

[5]National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment* (Washington, D.C.: National Academies Press, 2008). The report's preparation was overseen by the National Academy of Sciences Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals. Although the report addresses broader issues related to privacy and data mining, a senior National Research Council official stated that the committee included behavior detection as a focus because any behavior detection program could have privacy implications.

[6]For the purposes of this testimony, the term "TSA-regulated airport" refers to a U.S. airport operating under a TSA-approved security program and subject to TSA regulation and oversight. See 49 C.F.R. pt. 1542.

including efforts to validate the scientific basis for the program. As part of our efforts to update this information, we analyzed DHS's April 2011 SPOT validation study and discussed its findings with cognizant DHS officials.

For our September 2009 report on TSA efforts to secure airport perimeters and access controls, we examined TSA documents related to risk assessments, airport security programs, and risk management. We also interviewed TSA, airport, and industry association officials and conducted site visits at nine TSA-regulated airports of varying size.[7] We selectively updated the information in the report on risk management in July 2011.

For our July 2011 report on checked baggage systems, we compared requirements for explosives detection systems (EDS) established by TSA in 2010 and compared them to requirements previously established in 2005 and 1998 to determine how they differed.[8] To identify challenges TSA is experiencing in implementing the current EDS acquisition, we analyzed documentation from the Electronic Baggage Screening Program, including the acquisition strategy and risk management plans. We also interviewed TSA program officials regarding their approach to the current EDS acquisition, including revisions to plans and timelines. Our previously published products contain additional details on the scope and methodology, including data reliability, for these reviews.

All of our work was conducted in accordance with generally accepted government auditing standards. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis of 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. For new information that was based on work not previously reported, we obtained TSA views on our findings and incorporated technical comments where appropriate.

[7]See GAO-09-399.

[8]See GAO-11-740.

Background

The Aviation and Transportation Security Act established TSA as the federal agency with primary responsibility for securing the nation's civil aviation system, which includes the screening of all passenger and property transported by commercial passenger aircraft.[9] At the 463 TSA-regulated airports in the U.S., prior to boarding an aircraft, all passengers, their accessible property, and their checked baggage are screened pursuant to TSA-established procedures, which include passengers passing through security checkpoints where they and their identification documents are checked by transportation security officers (TSO) and other TSA employees or by private sector screeners under TSA's Screening Partnership Program.[10] Airport operators, however, are directly responsible 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 behavior detection officers (BDOs), who examine passenger behaviors and appearances to identify passengers who might pose a potential security risk at TSA-regulated airports;[11] travel document checkers, who examine tickets, passports, and other forms of identification; TSOs responsible for screening passengers and their carry-on baggage at passenger checkpoints, using x-ray equipment, magnetometers, Advanced Imaging Technology, and other devices; random employee screening; and checked baggage screening systems.[12] Other security layers cited by TSA include, among others; intelligence gathering and

[9]See Pub. L. No. 107-71, 115 Stat. 597 (2001). For purposes of this testimony, "commercial passenger aircraft" refers to a U.S. or foreign-based air carrier operating under TSA-approved security programs with regularly scheduled passenger operations to or from a U.S. airport.

[10]Private-sector screeners under contract to and overseen by TSA, and not TSOs, perform screening activities at airports participating in TSA's Screening Partnership Program. According to TSA, 16 airports participate in the program as of July 2011. See 49 U.S.C. § 44920.

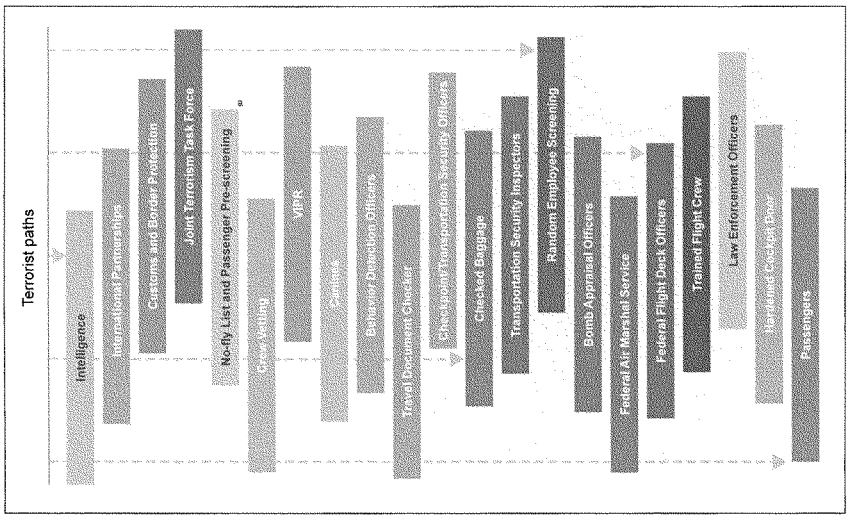
[11]TSA designed SPOT to provide BDOs with a means of identifying persons who may pose a potential security risk at TSA-regulated airports by focusing on behaviors and appearances that deviate from an established baseline and that may be indicative of stress, fear, or deception.

[12]Advanced Imaging Technology screens passengers for metallic and non-metallic threats including weapons, explosives, and other objects concealed under layers of clothing.

analysis; passenger prescreening against terrorist watchlists; random canine team searches at airports; federal air marshals, who provide federal law enforcement presence on selected flights operated by U.S. air carriers; Visible Intermodal Protection Response (VIPR) teams; reinforced cockpit doors; the passengers themselves; as well as other measures both visible and invisible to the public. Figure 1 shows TSA's layers of aviation security. TSA has also implemented a variety of programs and protective actions to strengthen airport perimeters and access to sensitive areas of the airport, including conducting additional employee background checks and assessing different biometric-identification technologies.[13] Airport perimeter and access control security is intended to prevent unauthorized access into secure areas of an airport—either from outside or within the airport complex.

[13]Biometrics are measurements of an individual's unique characteristics, such as fingerprints, irises, and facial characteristics, used to verify identity.

Figure 1: TSA's Layers of Security



Source: TSA.

[a]The No-Fly List is used to identify individuals who are to be prevented from boarding an aircraft while the Selectee List, another aspect of passenger prescreening, is used to identify individuals required to undergo additional screening before being permitted to board an aircraft. The No Fly and Selectee lists are derived from the consolidated terrorist watchlist maintained by the Federal Bureau of Investigation's Terrorist Screening Center.

According to TSA, each one of these layers alone is capable of stopping a terrorist attack. TSA states that the security layers in combination multiply their value, creating a much stronger system, and that a terrorist who has to overcome multiple security layers to carry out an attack is more likely to be preempted, deterred, or to fail during the attempt.

Behavior Detection Program

TSA has taken actions to validate the science underlying its behavior detection program, but more work remains. We reported in May 2010 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.[14] DHS's 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 identifying high-risk travelers.[15] However, as noted in the study, the assessment was an initial validation step, but 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. According to DHS, further research will be needed to comprehensively validate the program.

According to TSA, SPOT was deployed before a scientific validation of the program was completed to help address potential threats to the aviation system, such as those posed by suicide bombers. TSA also stated that the program was based upon scientific research available at the time regarding human behaviors. We reported in May 2010 that approximately 14,000 passengers were referred to law enforcement officers under SPOT from May 2004 through August 2008.[16] Of these passengers, 1,083 were arrested for various reasons, including being illegal aliens (39 percent), having outstanding warrants (19 percent), and possessing fraudulent documents (15 percent). The remaining 27 percent were related to other reasons for arrest. As noted in our May 2010 report, SPOT officials told us that it is not known if the SPOT program has ever resulted in the arrest of anyone who is a terrorist, or who was planning to engage in terrorist-related activity. According to TSA, SPOT referred about 50,000 passengers for additional screening in fiscal year 2010 resulting in about 3,600 referrals to law enforcement officers. These

[14]See GAO-10-763.

[15]See DHS, *SPOT Referral Report Validation Study Final Report Volume I: Technical Report*, (Washington, D.C.: April 5, 2011). DHS's study defines high-risk passengers as travelers that 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 that were ultimately arrested by law enforcement.

[16]See GAO-10-763.

referrals 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. DHS has requested about $254 million in fiscal year 2012 for the SPOT program, which would support an additional 350 (or 175 full-time equivalent) BDOs. If TSA receives its requested appropriation, TSA will be in a position to have invested about $1 billion in the SPOT program since fiscal year 2007.

A 2008 report issued by the National Research Council of the National Academy of Sciences stated that the scientific evidence for behavioral monitoring is preliminary in nature.[17] The report also noted that an information-based program, such as a behavior detection program, should first determine if a scientific foundation exists and use scientifically valid criteria to evaluate its effectiveness before deployment. The report added that such programs should have a sound experimental basis and that the documentation on the program's effectiveness should be reviewed by an independent entity capable of evaluating the supporting scientific evidence.[18]

As we reported in May 2010, an independent panel of experts could help DHS develop a comprehensive methodology to determine if the SPOT program is based on valid scientific principles that can be effectively applied in an airport environment for counterterrorism purposes. Thus, we recommended that the Secretary of Homeland Security convene an independent panel of experts to review the methodology of the validation study on the SPOT program being conducted to determine whether the study's methodology is sufficiently comprehensive to validate the SPOT program. We also recommended that this assessment include appropriate input from other federal agencies with expertise in behavior detection and relevant subject matter experts.[19] DHS concurred and

[17]Specifically, the report states that the scientific support for linkages between behavioral and physiological markers and mental state is strongest for elementary states, such as simple emotions; weak for more complex states, such as deception; and nonexistent for highly complex states, such as when individuals hold terrorist intent and beliefs.

[18]A study performed by the JASON Program Office raised similar concerns. The JASON Program Office is an independent scientific advisory group that provides consulting services to the U.S. government on matters of defense science and technology.

[19]See GAO-10-763.

stated that its validation study, completed in April 2011, included an independent review of the study with input from a broad range of federal agencies and relevant experts, including those from academia.

DHS's validation study found that SPOT was more effective than random screening to varying degrees. For example, the study found that SPOT was more effective than random screening at identifying individuals who possessed fraudulent documents and identifying individuals who law enforcement officers ultimately arrested.[20] According to DHS's study, no other counterterrorism or screening program incorporating behavior- and appearance-based indicators is known to have been subjected to such a rigorous, systematic evaluation of its screening accuracy. However, DHS noted that the identification of such high-risk passengers was rare in both the SPOT and random tests. In addition, DHS determined that the base rate, or frequency, of SPOT behavioral indicators observed by TSA to detect suspicious passengers was very low and that these observed indicators were highly varied across the traveling public. Although details about DHS's findings related to these indicators are sensitive security information, the low base rate and high variability of traveler behaviors highlights the challenge that TSA faces in effectively implementing a standardized list of SPOT behavioral indicators.

In addition, DHS outlined several limitations to the study. For example, the study noted that BDOs were aware of whether individuals they were screening were referred to them as the result of identified SPOT indicators or random selection. DHS stated that this had the potential to introduce bias into the assessment. DHS also noted that SPOT data from January 2006 through October 2010 were used in its analysis of behavioral indicators even though questions about the reliability of the data exist.[21] In May 2010, we reported weaknesses in TSA's process for maintaining operational data from the SPOT program database. Specifically, the SPOT database did not have computerized edit checks built into the system to review the format, existence, and reasonableness of data. Because of these data-related issues, we reported that

[20]The extent to which SPOT is more effective than random at identifying fraudulent documents and individuals ultimately arrested by law enforcement officers is deemed sensitive security information by TSA.

[21]DHS officials stated that this historical SPOT data was not used in their analysis to determine whether SPOT was more effective than random screening.

meaningful analyses could not be conducted to determine if there is an association between certain behaviors and the likelihood that a person displaying certain behaviors would be referred to a law enforcement officer or whether any behavior or combination of behaviors could be used to distinguish deceptive from nondeceptive individuals. In our May 2010 report, we recommended that TSA establish controls for this SPOT data. DHS agreed and TSA has established additional data controls as part of its database upgrade. However, some of DHS's analysis used SPOT data recorded prior to these additional controls.

The study also noted that it was not designed to comprehensively validate whether SPOT can be used to reliably identify individuals in an airport environment who pose a security risk. The DHS study made recommendations related to strengthening the program and conducting a more comprehensive validation of whether the science can be used for counterterrorism purposes in the aviation environment.[22] Some of these recommendations, such as the need for a comprehensive program evaluation including a cost-benefit analysis, reiterate recommendations made in our prior work. As we reported in March 2011, Congress may wish to consider the study's results in making future funding decisions regarding the program.[23] TSA is currently reviewing the study's findings and assessing the steps needed to address DHS's recommendations. If TSA decides to implement the recommendations in the April 2011 DHS validation study, DHS may be years away from knowing whether there is a scientifically valid basis for using behavior detection techniques to help secure the aviation system against terrorist threats given that the initial study took about 4 years to complete.

Airport Perimeter and Access Controls

TSA has taken actions to strengthen airport perimeter and access controls security, but has not conducted a comprehensive risk assessment or developed a national strategy for airport security. We reported in September 2009 that TSA has implemented a variety of programs and actions since 2004 to improve and strengthen airport

[22]The study made recommendations related to SPOT in three areas: (1) future validation efforts; (2) comparing SPOT with other screening programs; and (3) broader program evaluation issues. TSA designated the specific details of these recommendations sensitive security information.

[23]See GAO, *Opportunities to Reduce Potential Duplication in Government Programs, Save Tax Dollars, and Enhance Revenue*, GAO-11-318SP (Washington, D.C.: Mar. 1, 2011).

perimeter and access controls security, including strengthening worker screening and improving access control technology.[24] For example, to better address the risks posed by airport workers, in 2007 TSA implemented a random worker screening program that has been used to enforce access procedures, such as ensuring workers display appropriate credentials and do not possess unauthorized items when entering secure areas. According to TSA officials, this program was developed to help counteract the potential vulnerability of airports to an insider attack—an attack from an airport worker with authorized access to secure areas. TSA has also expanded its requirements for conducting worker background checks and the population of individuals who are subject to these checks. For example, in 2007 TSA expanded requirements for name-based checks to all individuals seeking or holding airport-issued identification badges and in 2009 began requiring airports to renew all airport-identification media every 2 years. TSA also reported taking actions to identify and assess technologies to strengthen airport perimeter and access controls security, such as assisting the aviation industry and a federal aviation advisory committee in developing security standards for biometric access controls.

However, we reported in September 2009 that while TSA has taken actions to assess risk with respect to airport perimeter and access controls security, it had not conducted a comprehensive risk assessment based on assessments of threats, vulnerabilities, and consequences, as required by DHS's *National Infrastructure Protection Plan* (NIPP).[25] We further reported that without a full depiction of threats, vulnerabilities, and consequences, an organization's ability to establish priorities and make cost-effective security decisions is limited.[26] We recommended that TSA develop a comprehensive risk assessment, along with milestones for completing the assessment. DHS concurred with our recommendation and said it would include an assessment of airport perimeter and access control security risks as part of a comprehensive assessment for the transportation sector—the *Transportation Sector Security Risk*

[24]GAO-09-399.

[25]GAO-09-399. DHS developed the *NIPP* to guide risk assessment efforts and the protection of the nation's critical infrastructure, including airports.

[26]See GAO, *Transportation Security: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation*, GAO-09-492 (Washington, D.C.: Mar. 27, 2009).

Assessment (TSSRA). The *TSSRA*, published in July 2010, included an assessment of various risk-based scenarios related to airport perimeter security but did not consider the potential vulnerabilities of airports to an insider attack—the insider threat—which it recognized as a significant issue. In July 2011, TSA officials told us that the agency is developing a framework for insider risk that is to be included in the next iteration of the assessment, which TSA expected to be released at the end of calendar year 2011. Such action, if taken, would meet the intent of our recommendation.

We also recommended that, as part of a comprehensive risk assessment of airport perimeter and access controls security, TSA evaluate the need to conduct an assessment of security vulnerabilities at airports nationwide.[27] At the time of our review, TSA told us its primary measures for assessing the vulnerability of airports to attack were professional judgment and the collective results of joint vulnerability assessments (JVA) it conducts with the Federal Bureau of Investigation (FBI) for select—usually high-risk—airports.[28] Our analysis of TSA data showed that from fiscal years 2004 through 2008, TSA conducted JVAs at about 13 percent of the approximately 450 TSA-regulated airports that existed at that time, thus leaving about 87 percent of airports unassessed.[29] TSA has characterized U.S. airports as an interdependent system in which the security of all is affected or disrupted by the security of the weakest link.

[27]GAO-09-399.

[28]According to TSA officials, JVAs are assessments that teams of TSA special agents and other officials conduct jointly with the FBI, generally, as required by law, every 3 years for airports identified as high risk. See 49 U.S.C. § 44904(a)-(b). See also Pub. L. No. 104-264, § 310, 110 Stat. 3213, 3253 (1996) (establishing the requirement that the Federal Aviation Administration (FAA) and the FBI conduct joint threat and vulnerability assessments). Pursuant to ATSA, responsibility for conducting JVAs transferred from FAA to TSA. For more information on this issue, see GAO-09-399.

[29]From fiscal years 2004 through 2008 TSA conducted 67 JVAs at a total of 57 airports; 10 airports received 2 JVAs. TSA classifies the nation's airports into one of five categories (X, I, II, III, and IV) based on various factors such as the number of take-offs and landings annually, the extent of passenger screening at the airport, and other security considerations. In general, Category X airports have the largest number of passenger boardings and Category IV airports have the smallest. According to TSA data, of the 67 JVAs conducted at 57 airports from fiscal years 2004 through 2008, 58—or 87 percent—were Category X and I airports. Of the remaining 9 assessments, 6 were at Category II airports, 1 at a Category III airport, and 2 at Category IV airports. Since our September 2009 report was issued, the number of TSA-regulated airports has increased from approximately 450 to 463.

However, we reported that TSA officials could not explain to what extent the collective JVAs of specific airports constituted a reasonable systems-based assessment of vulnerability across airports nationwide. Moreover, TSA officials said that they did not know to what extent the 87 percent of commercial airports that had not received a JVA as of September 2009—most of which were smaller airports—were vulnerable to an intentional security breach. DHS concurred with our recommendation to assess the need for a vulnerability assessment of airports nationwide. TSA officials also stated that based on our review they intended to increase the number of JVAs conducted at Category II, III, and IV airports and that the resulting data would assist TSA in prioritizing the allocation of limited resources. Our analysis of TSA data showed that from fiscal year 2004 through July 1, 2011, TSA conducted JVAs at about 17 percent of the TSA-regulated airports that existed at that time, thus leaving about 83 percent of airports unassessed.[30] Since we issued our report in September 2009, TSA had not conducted JVAs at Category III and IV airports.[31] Further, TSA could not tell us to what extent it has studied the need to conduct JVAs of security vulnerabilities at airports nationwide.

We also reported in September 2009 that TSA's efforts to enhance the security of the nation's airports have not been guided by a national strategy that identifies key elements, such as goals, priorities, performance measures, and required resources.[32] To better ensure that airport stakeholders take a unified approach to airport security, we recommended that TSA develop a national strategy for airport security that incorporates key characteristics of effective security strategies, such as measurable goals and priorities. DHS concurred with this recommendation and stated that TSA would implement it by updating the *Transportation Systems-Sector Specific Plan* (TS-SSP), to be released in

[30]From fiscal year 2004 through July 1, 2011, TSA conducted 125 JVAs at 78 airports; 47 airports received more than one JVA during this time period.

[31]From fiscal year 2009 through July 1, 2011, TSA conducted 58 JVAs at a total of 56 airports; 2 airports received 2 JVAs. According to TSA data, of the 58 JVAs conducted, 47—or 88 percent—were at Category X and I airports; 7—12 percent—were conducted at Category II airports. TSA officials told us that since our report in September 2009 they have initiated a semi-annual report process that, in part, included a data analysis of the JVAs conducted at airports for the prior six months. The semi-annual report focuses on airport perimeter, terminal, critical infrastructure, airport operations, and airport services. Beginning in fiscal year 2011 the reports are to be developed on an annual basis. The reports are also used to direct future JVA efforts.

[32]GAO-09-399.

the summer of 2010.[33] In July 2011 TSA officials told us that a pre-publication version of the *TS-SSP* had been sent to Congress on June 29, 2011, and that DHS was in the process of finalizing the *TS-SSP* for publication, but a specific date had not been set for public release.

Checked Baggage Screening Systems

TSA has revised explosives detection requirements for checked baggage screening systems but faces challenges in deploying equipment that meet the requirements. Explosives represent a continuing threat to the checked baggage component of aviation security. TSA deploys EDS and explosives trace detection (ETD) machines to screen all checked baggage transported by U.S. and foreign air carriers departing from TSA-regulated airports in the United States. An EDS uses a computed tomography X-ray source that rotates around a bag, obtaining a large number of cross-sectional images that are integrated by a computer that automatically triggers an alarm when objects with the characteristic of explosives are detected. An ETD machine is used to chemically analyze trace materials after a human operator swabs checked baggage to identify any traces of explosive material. TSA seeks to ensure that checked baggage screening technology is capable of detecting explosives through its Electronic Baggage Screening Program, one of the largest acquisition programs within DHS. Under the program, TSA certifies and acquires systems used to screen checked baggage at 463 TSA-regulated airports throughout the United States. TSA certifies explosives detection-screening technologies to ensure they meet explosives detection requirements developed in conjunction with the DHS Science and Technology Directorate along with input from other agencies, such as the FBI and Department of Defense.

Our July 2011 report addressed TSA's efforts to enhance explosives detection requirements for checked-baggage screening technologies as well as TSA's efforts to ensure that currently deployed and newly acquired explosives detection technologies meet the enhanced requirements.[34] As highlighted in our July 2011 report, requirements for EDSs were established in 1998 and subsequently revised in 2005 and

[33]TSA developed the *TS-SSP* to conform to NIPP requirements, which required sector-specific agencies to develop strategic risk management frameworks for their sectors that aligned with *NIPP* guidance.

[34]See GAO-11-740.

2010 to better address the threats. Currently, checked baggage screening systems are not operating under the 2010 requirements. As of January 2011, some of the EDS in TSA's fleet are detecting explosives at the level established by the 2005 requirements.[35] Meanwhile, other EDS are configured to meet older requirements established in 1998, but include software to meet 2005 requirements. The remaining EDS are configured to meet 1998 requirements but lack the software or both the hardware and software that would enable them to detect at the levels established by the 2005 requirements. TSA plans to implement the revised requirements in a phased approach spanning several years.[36] The first phase, which includes implementation of the 2005 requirements, is scheduled to take years to fully implement and deploying EDS that meet 2010 requirements could prove difficult given that TSA did not begin deployment of EDS meeting 2005 requirements until 2009—4 years later.

We found that TSA did not have a plan to deploy and operate EDS to meet the most recent requirements and recommended, among other things, that TSA develop a plan to deploy EDS that meet the current EDS explosives detection requirements and ensure that new EDS, as well as those already deployed in airports, be operated at the levels established in those requirements. In addition, TSA has faced challenges in procuring the first 260 EDS to meet 2010 requirements. For example, due to the danger associated with certain explosives, TSA and DHS encountered challenges safely developing simulants and collecting data on the explosives' physical and chemical properties needed by vendors and agencies to develop detection software and test EDS prior to the current acquisition. Also, TSA's decision to pursue EDS procurement complicated both the data collection and procurement efforts, which resulted in a delay of over 7 months for the current acquisition. We recommended that TSA complete data collection for each phase of the 2010 EDS requirements prior to pursuing EDS procurements that meet those requirements to help TSA avoid additional schedule delays.

[35]TSA has designated the number of EDS at the 2005 requirement level sensitive security information.

[36]The specific details included in the 2010 EDS requirements, such as the physical characteristics and minimum masses of each of the explosive types that EDS machines must detect, are classified.

Our report also examined other key issues such as the extent to which TSA's approach to its current EDS acquisition meets best practices for schedules and cost estimates and included a review of TSA's plans for potential upgrades of deployed EDSs. The report contained six recommendations to TSA, including that the agency develop a plan to ensure that new EDSs, as well as those EDSs currently deployed in airports, operate at levels that meet revised requirements. DHS concurred with all of the recommendations and has subsequently outlined actions to implement them.

Chairman Chaffetz, Ranking Member Tierney, and Members of the Subcommittee, this concludes my statement. I look forward to answering any questions that you may have at this time.

GAO Contact and Staff Acknowledgments

For questions about this statement, please contact Stephen M. Lord at (202) 512-8777 or lords@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this testimony are David M. Bruno, Glenn Davis, and Steve Morris, Assistant Directors; Scott Behen; Ryan Consaul; Barbara Guffy; Tom Lombardi; Lara Miklozek; and Doug Sloane.

Mr. CHAFFETZ. We'll now recognize Mr. Orr. He's the airport director and operator of the Charlotte International Airport. We appreciate you being here, sir. You're recognized for 5 minutes.

STATEMENT OF TJ "JERRY" ORR

Mr. ORR. Mr. Chairman and members of the subcommittee, my name is Jerry Orr, and I'm the aviation director for the city of Charlotte, at the Charlotte airport. I have worked for 36 years in airport management and was a small business owner for 13 years before that. I'm here today to testify on airport perimeter security.

I have been critical of the performance of the TSA since its inception. I am not critical of its mission. I am critical of its measures. In my judgment, the effectiveness of the TSA is compromised by a rigid attitude of arrogance and bureaucracy.

In November of last year, the body of a young man was discovered in Milton, Massachusetts, and was thought to have fallen from an aircraft. I learned about a possible connection to Charlotte in the media and, therefore, reached out to our Federal security director. He did not want TSA to take the lead and instead recommended I ask our municipal police department to head up an investigation and TSA would assist them.

Ultimately, the available evidence could neither prove nor disprove that a security breach had actually occurred at Charlotte. The police and TSA theorized how the young man may have accessed an aircraft. They came up with a reasonable assumption about what might have happened that excludes entry through a checkpoint. But the report fails to acknowledge that they could not conclusively rule out this possibility because TSA had failed to preserve their surveillance video of the checkpoints, and some of it was lost.

I'm not saying that the young man came through a TSA checkpoint. What I am saying is that the TSA failed to even admit the possibility, and deflected attention elsewhere. This mentality serves to protect the Agency at the cost of real security needs.

The investigation focused national attention on airport perimeter security. In Charlotte we have 19 miles of 6-foot-high chain-link fence with three strands of barbed wire enclosing the airport. This fence meets all Federal requirements. We spend a half million dollars annually on maintaining the fence, all from the airport budget. We spend an additional $3 million on 75 personnel with perimeter security responsibilities. The fence is a deterrent. It says, keep out. However, the final line of security is the eyes and ears of the 20,000 people who work inside the fence.

TSA seems to believe that airports are automatically in violation of the regulations, even when they did everything they were obligated to do and it simply didn't work. To me, that's like saying that Customs and Border Protection itself is violating the law each time an illegal alien crosses into the United States.

Other examples of TSA's lack of a partnership, we recently asked TSA to explain their security basis and their legal authority for directing us to do something. But TSA failed or refused to respond or even acknowledge our questions.

TSA has conflicting roles in operational and regulatory capacities that are not kept separate. Having an Agency interpret the rules,

implement actions, and then judge their effectiveness, lends itself to the possibility of abuse.

I am confident that I am not the only airport operator with significant concerns about the effectiveness of TSA. An adversarial relationship between airports and the very Agency entrusted to help safeguard them is clearly detrimental to the goal of safety and security.

So what can be done to improve our ability to focus on the real needs of our Nation's airports? Congress should continue to support—its support of allowing airports to opt out of using TSA, and ensure that the bureaucracy does not throw up arbitrary roadblocks to discourage us from pursuing this alternative. Any entity working with airports and airlines to achieve security must do just that, work with them. TSA's current "because I say so" culture does not foster respect.

I also believe Congress should redirect some of the available funding for airport security from TSA directly to airports. The operator is most familiar with the airport's vulnerabilities and strengths and is well equipped to make effective enhancements.

Safety and security are always our number one priority. There can always be more security, but the challenge is to provide better security. We need to spend money where it counts, on things that matter. The path forward to optimal security needs to be reasonable and collaborative. If airports are given the resources we need and a true partner for security, the traveling public will be the beneficiary.

Mr. CHAFFETZ. Thank you, Mr. Orr.

[The prepared statement of Mr. Orr follows:]



United States House of Representatives
Committee on Oversight and Government Reform
Subcommittee on National Security, Homeland Defense, and Foreign Operations

Statement of T.J. Orr
Aviation Director, Charlotte Douglas International Airport

Good morning, Mr. Chairman and Members of the Subcommittee. My name is Jerry Orr and I am the Aviation Director for Charlotte Douglas International Airport in Charlotte, North Carolina. I have more than 36 years experience in airport management and I was a small business owner for 13 years before that. I thank you for the opportunity to testify today on airport perimeter security, especially since I built the Airport's original perimeter fence in 1974.

Charlotte Douglas International Airport (CLT) is owned and operated by the City of Charlotte. We are now the fastest growing airport in the country. We served more than 38 million passengers in 2010 and are ranked seventh in the nation in airport operations and eleventh in passengers. We have seven major carriers, fourteen regional carriers and three foreign flag carriers that together provide 701 daily flights from CLT. We have nonstop service to 138 destinations, including 36 international locations. CLT is also US Airways largest hub.

The airport's role in the transportation system is to provide an infrastructure platform upon which the private sector- airlines, rent-a-car companies, concessionaires, and others- operate their businesses. Those businesses serve 38 million passengers a year, provide 20,000 jobs inside the fence and produces more than $10 billion in annual economic impact. CLT is vested in this partnership. If those businesses succeed then we succeed. If they fail, then we fail. We want to be successful and security is a part of that success.

The four major problems I see with TSA are inefficiency, inflexible protocols, abuse of power, and a lack of separation of power. With these shortcomings, achieving security can be lost in the shuffle. Everyone knows I have been critical of the performance of the TSA since its inception. My views do not necessarily reflect the views of my employer but I believe they are consistent with most of the aviation industry.

CLT is recognized as a leader throughout the industry. In fact, we recently received one of the most prestigious awards for Airports in the world – The Eagle Award. Presented by the International Airport Transport Association, this award recognizes productivity, transparency and best value for money performance by airports. The winner's positive record on safety, environmental, operational and social issues is also considered. We are one of only five U.S. airports to have ever won this award and consider this a high honor.

This award reflects our goal: to deliver the highest quality product to the customer at the lowest possible cost. And this places us in a position of conflict with the TSA. We all joke about "Thousands Standing Around" but overstaffing is a serious issue. I learned at an early age from my father that if you assign four people to do a one person job you lose efficiency accountability, quality, and create confusion for the worker. This is why the TSA has been known to discover a suspicious bag and then retain the wrong bag and to discover a questionable person and then detain the wrong person.

Security is a burdensome necessity in today's world. There is no question about that. But our efforts and expenditures should be designed to leverage people and expenditures in other areas. The TSA is so focused on protocols that they often lose sight of what is reasonable or even necessary. There is a tremendous emphasis on doing it the same way every time everywhere. If you drive the same car the same route the same time every day I can eventually figure it out. The only person that benefits from everything being the same is the perpetrator. Security needs are dynamic and a security organization needs to be similarly flexible.

A contentious relationship between the airport operator and the TSA does not benefit the customer. If you cannot even talk to each other you cannot work together to improve security. It is not my intention to bore you with minutiae. However, I do intend to provide you with ample details that will demonstrate why I am concerned about TSA's efficacy.

The lack of partnership and communication with the TSA was most evident this past year as we struggled to deal with a tragic situation. In November 2010, the body of a young man was found in Milton, Massachusetts. Investigators suspect that this individual breached airport security and fell to his death from an aircraft. The handling of this situation marked the beginning of the end of CLT's working relationship with the TSA on a local level.

As Aviation Director, I was aware of a developing theory being discussed among Massachusetts investigators, the FAA, airlines and local police regarding this young man missing from his home in Charlotte. Investigators suspected that the youth may have gained access to an aircraft at CLT and stowed away in the wheel well, at which time his body and may have fallen from the aircraft on final approach to Boston Logan International Airport. I learned much of the details of the theory from a press event held by former District Attorney and current Congressman Keating several weeks after the death was discovered. Massachusetts officials had taken steps to notify Homeland Security due to the aviation aspect. I therefore would have expected, but never received, official notification of the presumed CLT connection from Homeland Security through TSA.

As a result of what I heard in the media, I reached out to our Federal Security Director (FSD) to discuss next steps. After considerable conversation, our FSD recommended I engage our local municipal police department to conduct a thorough criminal investigation. I questioned this recommendation. Why wouldn't the Transportation Security Administration take the lead? What if we learned that

charlotteairport.com | PO Box 19066 | Charlotte, NC 28219 | P: 704.359.4000 | F: 704.359.4030
Owned and operated by the City of Charlotte

this situation involved multiple airports? Wasn't there a protocol that should be followed?

I tried to correlate this situation to my 30 plus years of industry experience. When there is a threat on board an aircraft – the FBI responds and investigates. When there is an airplane crash – the NTSB responds and investigates. When a pilot makes an error on the airfield – the FAA responds and investigates. If it is believed there is a security breach at a major US airport - why shouldn't the TSA respond and investigate? I made no headway with the conversation and reluctantly agreed to ask our local police department to spearhead an investigation in which the TSA agreed to participate. At this moment, it was clear to me that the dynamic of our relationship had shifted.

It appeared that the TSA was more interested in avoiding responsibility than in genuinely trying to understand if and how security may have been implicated. Because of the lack of leadership, substantial misinformation circulated in the national news which understandably distressed the public. We were unable to respond to all the misstatements and we were suddenly very alone in what was quickly becoming national news.

Our local police department did complete their investigation with the full cooperation and assistance of local TSA. The available evidence could neither prove nor disprove that a security breach had actually occurred at CLT. No real conclusions could be made.

As part of the investigation, TSA and local police reviewed available video surveillance. Please note that I said available video surveillance. We have an elaborate camera system at the airport, some of which was provided through a TSA grant. The camera system infrastructure is owned by the Airport but all video data is owned, monitored and maintained by the TSA. TSA neglected to safeguard their video of passenger security checkpoints and employee access points from the date the young man went missing until after the 30-day archival threshold. While there was some video remaining, other video surveillance was inaccessible at the time TSA finally sought to preserve it.

The final investigative report outlines a theory of what may have occurred, a theory that excludes a breach at any TSA checkpoint. The assumption is plausible and may well be right. However, the report fails to note that there was insufficient evidence to conclusively exclude TSA checkpoints as a possible point of entry. In failing to require that the report explicitly acknowledge the incomplete availability of surveillance video of the checkpoints, it appears that TSA is more interested in avoiding scrutiny than in a fair and impartial review of all possibilities.

I appreciate local law enforcement's efforts to assist us during an unprecedented situation, but I do question some of their findings and recommendations. A municipal police department does not have the expertise to thoroughly conduct an investigation with national security ramifications, nor should they be expected to. For example, it was noted as an "identified concern" that CLT supplements its security and law enforcement personnel with a private security company. Was TSA

charlotteairport.com | PO Box 19066 | Charlotte, NC 28219 | P: 704.359.4000 | F: 704.359.4030
Owned and operated by the City of Charlotte

truly engaged? Isn't TSA a part of the Department of Homeland Security? Don't they know that the firm in question, GS4 Wackenhut is a well known, international agency that Homeland Security itself contracts with throughout the nation in various capacities, including assisting Customs and Border Protection?

I could continue with multiple examples of where I feel the TSA was disconnected during this analysis but I think you get the gist. True security needs are being lost in the current climate. The aviation industry is the cornerstone of our nation's transportation system. It is ever changing and adjusts to changing conditions as needed. It requires proactive thinking- not the reactive thinking which is the operating mantra of the TSA. Congressman William Keating is absolutely correct. We should not wait for another tragedy like this to occur before acting accordingly.

This presumed stowaway situation put airport perimeter fencing in the spotlight. At CLT, we have 19 miles of perimeter fencing. In many areas of the fence there is redundant fencing – in some cases up to three layers. We spend $500,000 annually on maintaining the fence and related gates - from our own budget, not from TSA funding. We also spend another $3.2 million on approximately 75 personnel that are responsible, at least in part, for perimeter security. In addition to dedicated law enforcement and airport operations personnel, each of the approximately 20,000 people working at CLT plays a key role in maintaining airport security. Each person is instructed when they obtain their access privilege badge that they are responsible for maintaining airport security. As a condition of keeping their badge, they are obligated to report anybody who is within the perimeter fence in an unauthorized capacity.

The fence does serve as a deterrent. It keeps wildlife outside of the airport. It provides a visual barrier and/or boundary. It serves as a clear delineation of the Airport perimeter in some cases, and for most people, it serves as a clear message to prevent trespassing. The perimeter fence does not represent total security. The fence alone does not insure perpetrators will stay outside the airport perimeter. Real security comes through a layered approach, of which the fence is one element. I see airport perimeter fencing as a baseline or minimum standard – not a single tool of prevention for those individuals who are truly determined to access an airport.

In CLT, we have a very good record when it comes to safety and security. We pride ourselves on being an industry leader. We also pride ourselves on being a good partner and have multiple examples of successful partnerships that include Fortune 500 companies, domestic and international airlines and numerous branches of the local, state and federal government. This single incident unfairly tarnished the reputation of our organization.

CLT faithfully meets or exceeds all the requirements of the federal regulations. If something goes wrong anyway, it does not mean that we have failed to follow the regulation. That would be like saying that Customs and Border Protection itself was in violation of the law whenever an illegal alien crosses into the United States. An adversarial relationship between airports and the very agency entrusted to help safeguard them is clearly detrimental to the goal of safety and security.

charlotteairport.com | PO Box 19066 | Charlotte, NC 28219 | P: 704.359.4000 | F: 704.359.4030
Owned and operated by the City of Charlotte

TSA's failure - or refusal - to communicate adversely affects Airport operations. A recent example is that TSA told us to terminate a certain activity. We wanted to know why. If there was a genuine security concern we wanted to understand what it was so we could fix it. We also wanted to know what their authority was to mandate the termination where the activity in question takes place outside the fence and outside the terminal. Other airports engage in the same activity and we wondered why we were being treated differently. We asked TSA these questions but they ignored us. On the contrary, TSA simply reiterated that we should comply without any explanation or even an acknowledgement that we had asked any questions. This kind of "because I told you so" culture does not foster trust, nor does it foster an effective partnership for optimal security.

TSA's lack of responsiveness and failure to communicate has also affected our Airport Security Program. TSA has to approve the Airport Security Program, or "ASP", at all airports. We have been trying to get revisions to ours approved for about a year now. In July 2010, we submitted proposed revisions to our ASP to the TSA's Assistant Federal Security Director for Inspections. He gave us feedback in February 2011 and we resubmitted our revisions based on his guidance in early April 2011. Within about a week of that, he disappeared and an Acting AFSD for Inspections appeared. A month later, in mid-May, the Acting AFSD told my staff that he wanted us to totally rewrite our ASP- but then admitted that he hadn't read it. I say this not to point the finger at an individual, but to point out that the edict seems more about appearances than security. Why would someone who wasn't familiar with our airport and hadn't even read our ASP tell us it had to be totally changed? Was this a directive from above? If so, had whomever issued the edict actually read our ASP?

Since 2003, and approximately eleven times, we have easily and efficiently made necessary updates to our ASP with TSA's assistance and approval. Suddenly, however, our proposed twelfth version has been awaiting approval for almost a year. We still haven't been told what TSA is looking for. Two months ago the Acting AFSD told my staff he would get comments on our ASP back to us, but we have yet to receive them. In the meantime, we have sought to amend specific aspects of how we handle security and we do not know what TSA's position on it is or will be. We don't know who will make the decision. The ASP is our guiding security document. We have been left in a precarious position not of our own making. TSA's lack of responsiveness and bureaucratic confusion undermines CLT's security efforts.

Since the tragedy that led to the understandably significant attention by the media, I feel that CLT has been singled out for disparate treatment- even retribution-by the TSA. I imagine that TSA's attention will not decrease after my speaking out here today. I imagine getting CLT's revised ASP approved may become more, rather than less, difficult.

Despite CLT's particular situation, I am confident, as mentioned earlier, that I am not the only airport operator with significant concerns about the effectiveness of TSA. Where TSA has become an adversary rather than a partner for security, real needs are being lost. So what can be done to improve our ability to focus on the

charlotteairport.com | PO Box 19066 | Charlotte, NC 28219 | P: 704.359.4000 | F: 704.359.4030
Owned and operated by the City of Charlotte

real needs related to ensuring safety and security at our nation's airports and in the skies?

Congress should continue its support of allowing airports to opt out of using the TSA and ensure that roadblocks are not thrown in our way to do so. Any entity working with airports and airlines to achieve security must be willing to do just that- work with them. Communication, trust, and leadership are required.

When you ask an agency to explain a security concern is and they refuse to do so, they must think they are not your partner in achieving security. When you ask an agency to explain their legal authority for something they have requested of you and they refuse to answer, they must think they are all powerful. Having an agency that interprets the rules, implements the rules, and then judges their effectiveness lends itself to this kind of culture. TSA has both an operational and regulatory function and those conflicting roles are not kept well separated like they are in, for example, the FAA. This may be a contributing factor to TSA's overbearing treatment of airports and airlines.

I also believe Congress should redirect some of the available funding for airport security from TSA directly to airports. One size does not fit all. Every airport is different in many ways: location, geography, numbers of passengers departing or just passing through, etc. Each airport operator is intimately familiar with its vulnerabilities as well as its strengths and can therefore make effective enhancements and improvements.

There can always be more security; the challenge is to provide better security. We need to spend money where it counts, on things that matter. The path forward to optimal security must be reasonable, proactive, and cooperative. Common sense must prevail. If airports are given the resources we need and a true partner for security, the travelling public can only benefit.

charlotteairport.com | PO Box 19066 | Charlotte, NC 28219 | P: 704.359.4000 | F: 704.359.4030
Owned and operated by the City of Charlotte

Mr. CHAFFETZ. We'll now recognize Mr. Rafi Ron, the former director of security at Tel Aviv's Ben-Gurion Airport. Mr. Ron, you're recognize for 5 minutes.

STATEMENT OF RAFI RON

Mr. RON. Thank you, Mr. Chairman and members of the committee, for inviting me to testify today. I'd like to draw the committee's attention to three factors that I believe they are playing a key role in many of the shortcomings in airport security.

The first one is the imbalance that was created shortly after 9/11 when the TSA had the overwhelming task of recruiting, training, and installing technology in airports around the country, something that has tended to be the backbone of the TSA operation and influence over security at the airports. At the same time, the airport facility security has received much less attention, and not only that of screening of passengers and bags where most of the attention and the funding went into, but it was also executed according to the law by TSA, while the rest of it was left for the local authorities to take care of. Funding was relatively short. The standards for performance of the security task on the local level are not very clear and in many cases, do not even exist.

And the point of—or the issue of perimeter security is a very good example for that, because I think that traveling around the country, one can easily notice that, first of all, there is very little consistency in our airports as far as perimeter security is concerned. Second, most of our airports today are still not protected by an operating perimeter intrusion detection systems. In other terms, we don't know when a breach occurs. We get to know that only when it is addressed by somebody or when we end up with a stowaway making his way to the wheel well and, sadly enough, losing his life after takeoff. And obviously, this is not a good reasonable standard compared to those that we implement on the passenger and bag screening operation.

The other aspect of that is that the issue of jurisdiction is not very clear. When it comes to the security operation, security facility operation at the airport, by law it is the local law enforcement agency or department that is responsible to do this. But, yet, most or many of the police departments that provide that service in airports are still implementing their own more as a law enforcement agency rather than a security agency, and there is a major difference between the two.

And once again, if you look at perimeter as a reflection of this problem, you can see that the role that the local police department is taking on perimeter security at airports is minimal and is usually based on responding to calls rather than the early detection and the prevention.

So I think that there are two areas that still need to receive much more attention. One is the role and the funding of the local authorities as far as the airport facility security is concerned. And second, the need for standards that will create consistent, high-level performance that will characterize the security in airports around the country. I thank you very much.

Mr. CHAFFETZ. Thank you, Mr. Ron.

[The prepared statement of Mr. Ron follows:]

STATEMENT BY RAFI RON
PRESIDENT OF NEW-AGE SECURITY SOLUTIONS INC.
TO THE HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORMS
SUBCOMMITTEE ON NATIONAL SECURITY,HOMELAND DEFENSE AND FOREIGN OPERATIONS

July 13th , 2011

Good morning, Mr. Chairman and members of the Subcommittee. First, let me thank the Committee for inviting me to testify concerning airport perimeter security.

I am Rafi Ron, President of New Age Security Solutions (NASS), a transportation security consulting firm based in Dulles, VA. The company was established in the wake of the 9/11 disaster to provide more effective security solutions to airports, government agencies, and private transportation companies. Over the last nine years, we have supported numerous projects in the US and abroad involving airports, seaports and ground transportation.

Prior to founding NASS, I served as Director of Security at Tel-Aviv Ben-Gurion International Airport for a period of five years. In this position I was responsible for all aspects of the security operation and coordinating with my counterparts at airports around the world. My previous experience included more than 30 years in the field of security, intelligence, and counterterrorism for the government of Israel.

Experience has demonstrated that transportation systems in general, and aviation facilities in particular, have become high-priority targets for terrorist and terrorist organizations. Such systems constitute a critical portion of our infrastructure, without which our modern societies cannot function. Every indication is that these systems will remain high-risk venues in the foreseeable future. Unfortunately, key links in our transportation systems remain vulnerable to attack. Potential damages include not only a large number of casualties but also significant residual delays with major economic and political repercussions. Few other systems carry a higher level of vulnerability, with so many potential targets for terrorists seeking to act against the interests of the United States.

Since the 9/11 attacks, aviation security has received a great deal of attention. Enormous resources have been dedicated to improving the system. In that time, the US has become a driving force in making the international aviation system safer. Unquestionably, American aviation has become a harder target for terrorists to exploit. The terrorists, however, have been unwilling to abandon their goals. Instead, they have found new ways to threaten the traveling public. Consequently, we must continue to identify vulnerabilities and mitigate them before terrorist take advantage of them. The question is, "What airport security investments will pay the highest dividends?"

I would like to focus on three points:

- The institutional response to the 9/11 attacks;
- The the imbalanced allocation of attention and resource between direct and indirect security threats; and
- The misalignment between federal, state, and local jurisdictional goals.

First Response

The 9/11 attack required swift measures to be taken to improve aviation security. Congress addressed this need by passing the Aviation and Transportation Security Act (ATSA) that created the Transportation Security Administration. Under the act, TSA was charged with performing passengers and bag screening as well as regulating other measures necessary to maintain a secure aviation system.

TSA set about to create a national screening system by hiring and training 60,000 federal employees in approximately twelve months, one of the largest non-military federal employment efforts in history. At the same time they focused on acquiring and encouraging the development of state of the art technology to screen passengers and bags. Billions of dollars were spent and are continuing to be spent on those two security features. But even the federal government has limits. With the concentration on passenger and bag screening, other aspects of security have been relegated to "the back seat," receiving less attention and little funding.

The large federal investment and the relatively small state and local investment has resulted in unbalanced security airpot systems. Much less attention has been devoted to other layers of security such as perimeter protection, access control, and terminal security.

The system can be described as a house with a multimillion dollar burglar alarm on the front door, surrounded by a 24 hour a day security team, while the walls and the back doors remain largely unsecured and unguarded. As it stands today, the vast majority of commercial airports in this country, including some of the high profile airports, do not have the capabilities to detect and prevent an intruder from entering the airside of the airport through the fence or an adjacent waterfront. Very few airports have an operational Perimeter Intrusion Detection System (PIDS).

We continue to learn frequently about perimeter breaches. Some of those breaches result in unauthorized access to the same aircrafts we protect by the expensive checkpoint and bag screening operations. In November of last year, a 16 year-old young man lost his life as a stowaway in the wheel well of a US Airways plane bound for Boston. The tragedy started with a perimeter breach at the Charlotte, North Carolina airport. Unfortunately, this is just the tip of a much bigger iceberg concerning unmitigated airport vulnerability.

Jurisdictional Conflict

There is a related jurisdiction issue that makes the situation even more difficult. While screening is carried out and fully funded by the TSA, other security measures at the airport are not (with the exception of limited federal grant programs). Airport facility security is performed and

funded mostly by state and or local authorities.

This results in two main shortcomings: The first is a vague division of responsibilities between the airport authority, local law enforcement agencies, and the TSA. Depending on the nature of the security concern at any given time, one or more the agencies may be called on to respond. Although they have some degree of coordination, no one person at the airport is in charge of security and proactive programs may be undertaken or skipped by any of the three without consulting the others.

The second consequence of this diverse responsibility is that each airport throughout the country and each of the agencies at a given airport do not place the same priority on security, commercial, and operational considerations. For a local government, where the airport is the lifeblood of their tourist economy, they may be focused on making sure passengers have a high quality travel experience. For law enforcement their resource allocation may be in response to a crime in progress rather than anticipating terrorist actions. And the Federal Government may be much more focused on passengers and baggage than unsecured gates or fences at the end of a distant runway or those surrounding an aviation fuel farm.

Lack of Standards

A lack of clear standards, combined with funding shortages have forced many airports to operate at the minimum local legal threshold. The problem is not limited to perimeter security. It poses significant risks concerning terminal security and other airport security vulnerabilities. Local law enforcement protection, based on locally defined standards, in many cases results in treating airports according to traditional law enforcement for a non-airport environment. But the risks at an airport are different than for a library, a water treatment plant, or a courthouse. And under local standards, airports compete directly for shrinking local budgets dollars and the demands on local law enforcement personnel. An example of inadequate standards is the absence of a building code for blast protection. This could address building materials, offset distances, or security procedures. Many of our airport terminals, including the newly built ones, are vulnerable to car bombs and other suicide attacks with potential catastrophic results.

Summary

The lack of comprehensive approach to airport security leads to unbalanced and insufficient airport security operation. Gaps in airport security exist in many of the areas beyond TSA screening. Among them are: perimeter protection, access control, and terminal security. Mitigation of most of these vulnerabilities can be addressed by implementing the following measures:

- Establish incentives and avenues for each airport to create a clear, integrated, and harmonized organizational structure. Provide for partnerships that integrate federal programs, local law enforcement priorities, and the airport authorities goals. Such an integrated structure will prevent gaps created by the existing fragmented approach.

- Task TSA with developing comprehensive, integrated airport security models that

include design, technical systems, operational elements, and human resources factors. Then allow each airport security partnership to adopt an integrated model that responds to its individual circumstances.

- Develop standards based on the above models that cover all aspects of airport security. These standards should be enforced through federal funding, regulatory programs, and periodic supervision.

- Create clear goals for local law enforcement agencies in addressing their counter terrorist role at airports. Support these goals by providing dedicated funding for staffing, training, and equipment.

- Reallocate federal aviation security funding to support local airports in their efforts to develop comprehensive security measures that will improve passenger security.

Thank you for your consideration.

Mr. CHAFFETZ. A little bit of explanation here as we introduce Inspector Parker. You may be curious as to why we would invite somebody from Amtrak, Amtrak Police to be here at the hearing regarding airport security. One of the questions, I think, that is a legitimate one that this committee would like to explore is, while the TSA has invested hundreds of millions of dollars in whole body imaging machines and technology, there are those, particularly at the Pentagon, that have come to the conclusion that dogs are the single best way to find explosive devices.

I'd like to ask unanimous consent to introduce in the record—there was a press conference by Lieutenant General Michael Oats. It says, "Dogs are the best detectors." And this, I would point to this, I know all good Americans get this magazine, Airman, which is the magazine of the U.S. Air Force. In their May/June 2011 edition, this little pull-out quote here says, "There's no technology proven more effective in the detection of explosives than the K–9."

And there are questions as to are we investing enough in technology that we know that works in K–9s, according to the Pentagon, having spent literally tens of billions of dollars.

So, again, without waxing on too much more, we do truly appreciate Inspector Parker being here. And as just a bit of explanation, he's going to give a bit of testimony and then we're going to have a demonstration. Don't let anybody in here worry anybody in here. But I'll let him explain how we're going to conduct this.

We would just ask that anybody here in the audience stay put, and if you have some sort of, you know, something, we're glad that you're here, Inspector Parker. But we're going to do a bit of a demonstration. We just ask that you kind of hang tight while we do this demonstration, and appreciate the leeway here of the committee as we do this demonstration. Inspector Parker, we'll give you great leeway for your testimony.

STATEMENT OF WILLIAM PARKER

Mr. PARKER. Good morning, Mr. Chairman and Ranking Member Tierney. My name is William Parker, and I'm the inspector commander of the Amtrak Police Department's K–9 unit. I'm honored to be here today, and I appreciate the invitation to speak with you about what dogs can do to improve airport security and detect explosives.

A well-trained dog is more capable, useful, reliable and effective than equipment. Dogs do not depreciate like machines do. If dogs are trained properly and if their training is consistent, their skill level will increase with experience.

Perimeter security is of great concern to airports and the Transportation Security Administration. Many airports rely on surveillance beams and cameras to protect their perimeter. The problem is, if nothing appears on the camera after the alarm goes off, you can't just assume nothing's there. Someone has to respond and make sure no one is hiding from the camera.

A well-trained law enforcement officer with a well-trained patrol dog can find and address that threat immediately without waiting for backup.

On and after September 11, 2001, we used explosive dogs intensively to sweep airport terminals. The dogs were used to sweep for

explosives in the morning before the terminal opened and in the evening when the terminal closed. I saw a real surge in interest in K–9s' capability after 9/11 as people realized dogs were effective in crowded environments where their explosive screening abilities were better in crowds than technology.

At Amtrak, trains are randomly swept for explosives before boarding. We keep an explosive team present at the boarding gates to provide a detection capability and immediate response.

I think a dog on a jetway at boarding would improve security at no inconvenience to travelers, and would provide an elevated sense of security. Dogs are very effective not only in detecting explosives, but as a deterrent in many environments, any environment when deployed properly.

Amtrak has many challenges as airport authorities, particularly the need to secure open-space areas that intruders could use to come into our property. We have been able to implement some new procedures that could be used in airports. I have helped pioneer a new application of K–9 called "vapor wake." Vapor wake is a dog trained to smell the wake of explosives and material in the air after a person passed by that area. Amtrak is working with Auburn University and other agencies to develop this application, and other agencies such as TSA are starting to use vapor wake K–9 methods.

In closing, I would like to reiterate my position that a K–9 program is an excellent investment for any agency that needs to secure high-traffic areas or facility perimeter, provided the program is properly funded and supported with a strong infrastructure.

[The prepared statement of Mr. Parker follows:]

Good morning, Mr. Chairman and Ranking Member Tierney, my name is William Parker, and I am the Inspector/Commander of the Amtrak Police Department's Canine Unit. I am honored to be here today, and I appreciate the invitation to testify before you on the topic of airport perimeter security.

Prior to joining Amtrak four years ago, I worked for the Metropolitan Washington Airports Authority, with responsibility for K-9 teams at Dulles International and Reagan National Airports. I'm also a retired Army Military Police Non-commissioned Officer.

While on active duty, I was a US Army Certification Authority for working dogs. I have also contributed my expertise to implementation of canine programs during my 20 years of service with the U.S. Army. I was selected as one of the Army's first Explosive Detection Dog team leaders to be deployed in support of Operation Desert Shield. As Kennel Master for the Military District of Washington from 1994 to 1997, I planned and coordinated all narcotic and explosive Detection dog missions in the Fort Myer Military Community and throughout the Military District of Washington. I provided on-call support to the Secret Service for the President, Vice President and visiting Heads of State. I established the training program for explosive and narcotic Detection dogs for Fort Myer and other civilian law enforcement agencies. Most of my military career was spent working to secure facilities – including air and rail infrastructure – and perimeters of military installations in the U.S. and abroad.

I am also highly decorated for:

- Coordinating and supervising 45 explosive detection dog teams during the 1996 Democratic National Convention in Chicago, Illinois,
- Department of Defense coordinator for 15 explosive Detection dog teams in support of the 1996 United Nations General Assembly 51 in New York, New York,
- Supervising 24 Detection dog teams in support of the 1997 Presidential Inauguration in Washington, D.C., and
- Supporting the 1990 Goodwill Games in Seattle, Washington.

I was hired by the Metropolitan Washington Airports Authority in 1997 to strategically plan for the start-up and management of a newly formed K-9 division for the Metropolitan Washington Airports Authority Police Department at both Dulles and Reagan Airports. At the time, the Airport Authority had **no** K-9 program of any kind. My role was to develop a K-9 program to support both airports and acquire the necessary training, equipment and facilities to support the program with the challenge of integrating the K-9 teams into daily airport operation. I developed the general orders of policies and procedures for explosive detection dog operations for both airports. I also assisted area engineers in the planning and coordination of a $600,000 kennel facility and implementing the training program for ten explosive detection dog teams, which secured two major airports. The decision to develop a program of this capability came directly from the recommendations of the White House Commission on Aviation Safety and Security,

which recommended the deployment of canine team assets at major Airports. To initiate the program, the government authorized $60,000 per team, per year, for the first two years of operation. The Authority initially deployed 8 teams for Dulles Airport and later added an additional 2 teams, which were used to expand coverage to Reagan National Airport.

In my current position with Amtrak I've supervised explosive detection dog teams at the last Presidential Inauguration, the Vancouver Olympics, and I have conducted demonstrations for many Federal agencies, including the TSA, CIA, FBI, Secret Service, and the Department of Defense to show the effectiveness of vapor wake detection canine teams capabilities.

I think it's important to emphasize some of the unique capabilities that a well-trained dog team can bring to the transportation environment that is primarily driven by technology. A dog is more capable, useful, reliable, and efficient than equipment. Dogs do not depreciate like machines do. If dogs are trained properly, and if their proficiency training is consistent, then their skill level increases with experience. Their natural abilities, when paired with a trained law enforcement officer, allow law enforcement to identify and address threats in real time. The need for such a capability has been recognized for more than a decade.

Perimeter security is of great concern to airports and the Transportation Security Administration. Many airports rely on surveillance beams and cameras to protect their perimeters. The problem with this procedure is that if nothing appears on the camera after an alarm goes off, you can't simply assume there's nothing there. You still need someone to respond and make sure no one is hiding from the camera. The K-9 team can respond more effectively than an individual police officer. Of course this type of K-9 would have to be a patrol dog and not an explosive detection dog team.

On and after September 11, 2001, we used dogs extensively to sweep the terminal as soon as we had successfully evacuated the area. The dogs were also used to sweep for explosives in the morning before the terminal opened and in the evening after the terminal closed. I saw a real surge in interest in K-9 capabilities after 9-11, as people realized that dogs were very effective in crowded environments where their explosive screening abilities are better suited to fast screening of large groups than technology is.

At Amtrak, trains are randomly swept before they are boarded, to ensure no explosive devices have been hidden on board. And we keep an explosive canine team present at boarding gates, to provide detection capability and immediate response. I think the presence of a dog team on a jetway at boarding would improve security at no additional inconvenience to travelers and would help to provide travelers an elevated sense of security. Dogs are very effective, not only as a means of detection, but also as a deterrent in any environment when deployed properly.

Amtrak has many of the same challenges as the Airports Authority, particularly the need to secure open spaces that intruders could use to enter the property. We have been able to establish some excellent working partnerships with TSA and Auburn University. Auburn works with us on our certification and on our annual two week advanced training course to improve our officers' dog-handling skills. I think we have been able to implement some procedures that

would be of great value, if they were adopted for airport use. For example, I have helped pioneer a new application for canines called "vapor wake." This capability allows a dog to detect the presence of explosive odor as it emanates off an individual into the air as they pass through an area. The "wake" of the explosive material in the air creates an opportunity for explosive detection. Amtrak continues to develop this capability with Auburn University and other agencies, such as TSA, are starting to adopt the vapor wake canine methodology.

In closing, I would like to reiterate my position that a good K-9 program is an excellent investment to deter terrorism for any agency challenged with securing a high-traffic area or a facility perimeter, provided the program is properly funded and supported with a strong infrastructure.

To make this point, I have brought 2 teams with me to give a brief demonstration. After we conclude the demo, I will be happy to answer any questions you might have.

Thank you again for this opportunity.

Mr. PARKER. To this point, I've brought two teams with me to give a brief demonstration. After we conclude the demo, I will be happy to answer any questions you might have. And thank you again for this opportunity.

What you are going to see in this demo, sir, is that—I explained to you about vapor wake technology. The dog will be able to detect people that walk by. It is not intrusive. They will not stop anybody's path.

You're going to see two—from my right, your left, we're going to have people come through the door. As you see the dog is like pretending she's at a checkpoint. People are going to come in and the dog is going to be able to detect who came in with something on them. We're just waiting on a crowd of people. These are your staffers.

As you see, sir, the dog is not intrusively hurting anybody walking. As you see now, that's a hit. As you see, that person walked by. The dog is walking. Stop decoy. As you see, this is a response that the dog would give. And that's a person, and this individual has ankle weights on that has explosives on his ankle. So you can look at him physically and not see anything, but he has about 5 pounds of explosives on his ankle.

Could you show the committee, sir? And in that is smokeless powder.

All right. The second demonstration we're going to give—okay. You can move. The second demonstration we're going to give is, like I say, when a person passes through an area. That's Levi, our chocolate Lab.

As a person passes through an area, you'll see a person walking through your room right there, over there to your left. She's going to walk and sit down. We're going to have a dog come through that same area. That person has already sat down. That dog is going to come in and follow the scent where the person walked to and determine where she's located at. They're just trying to give it a little bit of time because in theory, it's been known that somebody could walk through the area, and 15 minutes after they have passed through, the dog could still pick that up. And that's a scientific fact that's already been noted.

And that's Zeta coming in. Good girl. Let's give the dogs and handlers applause, sir.

Again, I want to thank you for this opportunity, and any questions you may have.

Mr. CHAFFETZ. Thank you. Very impressive. Appreciate it.

I'm now going to recognize myself for 5 minutes as we move the questioning. And we'll go from there.

I want to start with Mr. Sammon here and the GAO. The GAO in the report that's released out today, it's dated today, on page 12 and 13, it says, "Our analysis of TSA data show that from fiscal year 2004 through July 1, 2011, TSA conducted JVAs, or joint vulnerability assessments, at about 17 percent of TSA-regulated airports that existed at the time, thus leaving about 83 percent of airports unassessed. How can that be?

In 2009, September 2009, there was a report issued saying that 87 percent of the airports haven't been assessed. And over that

timeframe we've now only moved that number to 17 percent assessment?

Mr. SAMMON. The joint vulnerability assessments are done in concert with the FBI. They are done—they're extensive assessments. They are done in a limited number of locations, but every single commercial airport receives an annual security assessment.

Mr. CHAFFETZ. But wait, wait. Why aren't there 100 percent JVAs done, joint vulnerability assessments? Is the goal not to get to 100 percent?

Mr. SAMMON. TSA does complete security assessments, including the perimeter of all airports every year. Including—we've done 27,000 inspections.

Mr. CHAFFETZ. I'm asking about the joint vulnerability. I recognize they're different assessments.

Mr. SAMMON. There are different assessments, and it's a different assessment.

Mr. CHAFFETZ. What is your goal? Do you have the goal of getting to 100 percent? Yes or no?

Mr. SAMMON. We will not get to 100 percent of 450 airports with the FBI every year, no.

Mr. CHAFFETZ. Not even every year. At some point. I mean—okay. Mr. Lord, you've looked into this. What were your findings in this particular area?

Mr. LORD. When we first looked at it, the number was actually 13 percent. And that was from the 2004–2008 timeframe. And we asked TSA for some updated analysis. So the numbers have actually gone up. It's now 17 percent. These are very intensive examinations focused on high-risk airports, and TSA considers them the gold standard. They obviously conduct a whole host of other activities and inspections and testing. I mean, there's quite a few things they do. But you know, we thought this was worthwhile to single out, given the significance. We do recognize, you know, they're difficult to do quickly and you have to get the FBI involved. So it is a lot.

Mr. CHAFFETZ. What I don't understand is, given the imperative, given the knowledge and understanding that we're only as strong as the weakest link, and it may be that small airport, as we saw on 9/11 when that person got on a plane, not at one of the major, major airports initially, and got into the system, got behind the security line. Why is the TSA not demanding and working toward getting to 100 percent? I don't understand. There's 457 airports. Why aren't 457 airports getting this JVA done?

Mr. SAMMON. This level assessment will be done with a limited number of airports. Not all airports will be done. They will have inspections and they will have a complete assessment every year.

Mr. CHAFFETZ. I just, I absolutely don't understand that. I don't understand. I think it's unacceptable. Let me move on.

Mr. Orr, in your testimony, you said that the TSA has yet to approve this airport security program. I think you said in your testimony, "We have been trying to get revisions to our approval for about a year now." Can you explain that a little bit more, please?

Mr. ORR. Yes, sir. We're required to amend our security plan anytime there's a change in our security procedures. And we submitted an amendment to the local Federal Security Director over

a year ago; heard nothing for 6 or 7 months; got comment, addressed that comment. It again lay idle for a couple of months. And then our assistant security director that we had been working with disappeared and a new one appeared. And then the process started all over.

Mr. CHAFFETZ. Mr. Sammon, do you care to respond to that?

Mr. SAMMON. Yes. As I understand, the request to rewrite, to change the—amend the security plan—was in progress, was initiated about a year ago. There was a joint vulnerability assessment with the FBI conducted in the fall of 2010. It's my understanding—I don't know this personally—but it's my understanding the parties agreed to let's hold off on completing the rewriting of the airport security plan until we understand the results of the joint vulnerability assessment.

Now, the joint vulnerability assessment, in terms of its analysis of perimeter security, was not particularly flattering. And so in terms of where the amendment is, in terms of rewriting it, I think both parties agreed——

Mr. CHAFFETZ. Well, it sounds like he's been waiting for a year. Do you dispute that?

Mr. SAMMON. Both parties agreed to wait until—something you brought up last time is the joint vulnerability assessment, and that was an input. That should be very insightful in terms of what you do with your security plan.

Mr. CHAFFETZ. Mr. Orr.

Mr. ORR. We've had two joint vulnerability assessments, one in 2007 and one in 2010. At the conclusion of each one, we asked for additional information; help us to understand what you're talking about here, and in both cases have not received that. We submitted our plan, our amendment. We heard nothing. We checked on it a couple of times. They said it was in the works.

Mr. CHAFFETZ. And this is the frustration. You're telling me that you have no goal to get to 100 percent of joint vulnerability assessments on the 457 airports. You made improvement from 13 percent to 17 percent. And then we have an airport where you have done a JVA, a joint vulnerability assessment, and you're not getting the responsiveness. These should be collaborative efforts. You've got people all across the country. You're supposed to be the expert in the middle. That's my concern.

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

Mr. TIERNEY. Thank you very much. Mr. Lord, this joint vulnerability assessment, what's your analysis of how likely it is that 100 percent of the airports could undergo that particular scrutiny every year?

Mr. LORD. Well, we don't think that it would be appropriate to do every year, but perhaps on a rolling basis. That's how they do now. They have a target within a 3-year timeframe, they try to focus, you know, complete JVAs on the high-risk airports. It's a matter of resources but obviously they're expensive and you need to get the FBI's cooperation.

Mr. TIERNEY. Currently they're on a 3-year rolling plan to do 100 percent of the high-risk airports within that timeframe.

Mr. LORD. That would be difficult to achieve under the current process. I would defer to Mr. Sammon on that. He would know more about that.

Mr. TIERNEY. But it's your understanding that that's the plan.

Mr. LORD. It's not the plan. As Mr. Sammon stated, the current goal is not to do 100 percent. My point is they do them on a rolling 3-year basis.

Mr. TIERNEY. So Mr. Sammon, how many of those high-risk airports would be done on the rolling 3-year basis?

Mr. SAMMON. I'd have to get back to our operations people and get you an answer. I'm sure we'd be happy to respond to the committee on that.

Mr. TIERNEY. Would it be close to 100 percent? Would it be 50 percent? Would it be 25 percent?

Mr. SAMMON. I would have to check with the FBI. We need FBI cooperation. It's not a TSA event. Getting FBI resources, review of the project, sign-off, and so on and so forth; it's not a TSA—we don't run this thing by ourselves.

Mr. TIERNEY. Okay. Mr. Sammon, let me—what we were talking about, the Screening Passenger Observation Techniques program, the SPOT program, can you differentiate that from the usual type of random search?

Mr. SAMMON. Yes. Essentially I think your other witness on the panel, Mr. Ron, is an expert in this. But what you're looking for are microfacial anomalies in terms of the way people are behaving, particularly the kinds of facial movements they have as they approach the checkpoint. These SPOT programs resulted in more than 2,000 arrests since 2006, again, for people who had perhaps criminal and other kinds of fraudulent other illegal activities that they were engaged in.

But the science is based upon microfacial anomalies and the way that people look, and that's what they're trained to. So it's more than random. You're looking for people. You're looking at the crowd, looking for people who have, in that context, somewhat aberrant looks.

Mr. TIERNEY. Mr. Ron, we're about a billion dollars into this, or three-quarters of a billion dollars into a quarter we didn't ask for. Is that worth the money?

Mr. RON. Yes. I think that the investment in the behavior observation certainly makes sense because all the rest of what we are doing is very much limited to the detection of items. And I think 10 years after 9/11, with the attempted attacks that we had during this period of time, we reached the conclusion that we need to spend more attention on people rather than just on items. And observing behavior is one of the basic tools that can be used at the airport, but obviously it is only one single tool in a much wider and more complex strategy.

Mr. TIERNEY. What kind of technology is involved in the SPOT program?

Mr. RON. Well, it depends on the way you define technology. If we're looking at technology from the point of view of machines that are involved, or computers that are involved in the process. This is not a highly technological process. This is more a human-based process. But there's certainly room to expand that into the techno-

logical area by use of surveillance technology, and I mean smart surveillance technology, not just cameras out there, but those that can identify certain types of events or behavior and may help us respond to it in real time.

Mr. TIERNEY. So at the granular level, it could be done just with trained human beings exercising the process that's involved.

Mr. RON. Well, right now it is mostly training human beings, yes.

Mr. TIERNEY. Well, I would imagine when you start getting remote possibilities in there and technology for that, the cost would be enormous when you're talking about all the airports that are around.

Mr. RON. Yes, this is correct.

Mr. TIERNEY. Mr. Orr, I just want to, just real quickly, you talked about having the local entity be able to opt out of TSA on that. And if your organization did that, would you be willing to take the full responsibility and liability for failures to succeed?

Mr. ORR. Yes, sir. I have that anyway.

Mr. TIERNEY. All right. Good. I yield back.

Mr. CHAFFETZ. Thank you. I now recognize the chairman of the Transportation Committee, Mr. Mica of Florida.

Mr. MICA. Thank you. Mr. Sammon, you had as of last week, my figures are you had 3,905 people in Washington, supposedly working for TSA, and 27 percent of them were in a supervisory or an an administrative capacity, making on average, all of them, over $104,000.

How many of those folks were dedicated to doing the vulnerability assessments that we've been talking about here?

Mr. SAMMON. In terms of the vulnerability assessment, I would say a limited number. But we can get you the numbers.

Mr. MICA. How many?

Mr. SAMMON. I don't know, sir.

Mr. MICA. A dozen, half a dozen?

Mr. SAMMON. I'd have to get back to you. I'd like to give you a truthful answer.

Mr. MICA. Next you have 9,656 administrative personnel out in the field. How many of those folks are involved in the vulnerability assessment? Those are administrative people, not screeners.

Mr. SAMMON. I would have to give you the same answer in terms of responding to the committee.

Mr. MICA. And they are having trouble getting back with people like Mr. Orr I see because the FBI and other agencies don't cooperate. That is your explanation today?

Mr. SAMMON. No, sir. In terms of the ASP, I will look into it. I am not personally familiar——

Mr. MICA. You couldn't possibly have an FSD or some of the people who are making over $100,000, and maybe you could get for the record the number of people that are making over $100,000.

At Mr. Orr's airport, none of those people could check off on a security plan to protect the perimeter of the Charlotte Airport. Have you set the protocols and standards in Washington?

Mr. SAMMON. The plan is worked out locally with the airport director and the FSD. And it is approved through Washington.

Mr. MICA. But it takes 6 months to even get a response.

Mr. SAMMON. I think the JVA——

Mr. MICA. Can't you understand their frustration? The other thing, Mr. Orr, too, if anyone contacts you and there is any intimidation after your testifying here today, or any indication that they are giving you a hard time in any way, I want you to let this committee know immediately.

Mr. ORR. Yes, sir.

Mr. MICA. I have seen the way these people operate, the intimidation. I mean, you're pretty brave to be with us today. What is the current most serious risk that we face?

Mr. SAMMON. I think right now in terms of non-metallic explosives on airplanes coming in from overseas.

Mr. MICA. Okay. That is a good point. Actually, Mr. Pistole said that way back in November 2010, that we were in the risk management business, being a risk-based intelligence organization. That is what he is trying to achieve and I support that goal.

Do we have a plan from TSA that you could share with us to move toward that?

Mr. SAMMON. I don't have a plan today, but I would recommend the committee work with Administrator Pistole. His number two——

Mr. MICA. Can you provide us with an update from him on where you go—where you are going with that risk-based plan?

Mr. SAMMON. I will tell you that he is working on a number of alternatives and he hopes to announce something soon this summer.

Mr. MICA. But we are looking forward to that. And you mentioned that most of the risk is coming in from out of the United States. For example, Orly was the shoe bomber, Mr. Reid. Amsterdam, the diaper. Christmas Day bomber, the London liquid, the Yemen toner. The last count I had—well, we had under 100 TSA personnel overseas. It was really 54 when I checked. Do you know what the number is now?

Mr. SAMMON. I don't know off the top of my head.

Mr. MICA. Do you know if you had contact with the Secretary of State and others in trying to increase the presence of TSA overseas?

Mr. SAMMON. We work with overseas countries. We have people——

Mr. MICA. Would you provide the latest contacts with the Department of State and others to the committee on—because you said the threat is coming from there.

Now, whole body imaging equipment, which we spent a half a billion dollars on and the deployment of—I mean, we are probably in the billion-dollar range.

At this March 16th hearing, I asked the question: We know that terrorists are moving to body-cavity inserts with surgical implants. Does the whole body imaging equipment direct this kind of—can it detect this kind of threat? The answer from all of them, the experts, was that it does not.

Mr. SAMMON. It will depend. And I can't discuss it in this setting. It is classified. I would be happy to have a classified update.

Mr. MICA. They said that it did not. Now, we have known since—this is a BBC news release—that from 2009, September 2009, that

terrorists were now moving. In fact, they used a bomb on a terrorist implant and it blew up in front of a Saudi prince, killed himself. I mentioned this back in—what is the date? March. And that appears to be a threat, that they are moving.

Obviously they have gone from shoes, to diaper, to liquid, to cartridges. Wouldn't you say that it looks like the body implant might be a way to go?

Mr. SAMMON. I dispute that BBC report. But again, I can't discuss it in here. We could do it in a classified setting.

Mr. MICA. There is no dispute. He blew the crap out of the guy.

Mr. SAMMON. Sir—I will be happy to discuss it in a classified setting.

Mr. MICA. Well, in any event—and I mention this—and it was also mentioned that the equipment we spent a billion dollars on can't do anything about it. And TSA finally gets to July 6th, gets recently briefed air carriers and foreign partners to provide greater insights into intelligence indicating get you interested. There is terrorists to target aviation. And they name specifically the threat of body implants as a threat. Is that something you issue?

Mr. SAMMON. I would be happy to discuss the specifics of that in a classified setting, sir.

Mr. MICA. I mean, you can't tell me that you——

Mr. SAMMON. We have spoken with the airlines and talked to them about security procedures, yes, sir.

Mr. MICA. Did it take you to July to finally tell them, or did you tell them that this might pose a threat before then?

Mr. SAMMON. We have been working on non-metallic threats for the airlines for a considerable period of time. And this specific threat was based on specific intelligence that was put together——

Mr. MICA. And most of the testing of that equipment, both by this committee—directed by GAO has been unsuccessful both in reports that have been published and also in GAO reports that also look at your backup system, which is the SPOT program, which they termed almost a total failure——

Mr. SAMMON. I think Mr. Ron——

Mr. MICA [continuing]. In addressing this risk.

Mr. SAMMON. I totally disagree with you, in terms of what you are looking for are other alternatives to get around technology as people tend to try to design——

Mr. MICA. Are you aware of the hearing that was conducted by the Science and Technology Committee where Mr. Broun from Georgia, the chairman, questioned the use—the current application of standoff behavior detection, which you employ now, versus the active questioning, which is done under the Israeli system?

Mr. SAMMON. I think they are both very good.

Mr. MICA. Well, the—everyone who testified, every expert said that the TSA current procedure is a total failure and they further validated the findings of GAO.

Mr. SAMMON. I'm not familiar with the witnesses.

Mr. MICA. Again, I had the opportunity 2 weeks ago to be in Tel Aviv at Ben-Gurion Airport to see how it was done. And it can be done on an interactive basis, even with a large population, if we go to risk-based rather than hassling innocent Americans, veterans, military, children and people who pose absolutely no risk.

I yield back the balance of my time.

Mr. SAMMON. So I would encourage you to speak, to work with Administrator Pistole. Thank you.

Mr. CHAFFETZ. We try. You know, we try to get the senior most people to come before this committee and they refuse. And that is one of the great frustrations. That is no surprise to the TSA. I would love to work with them, love to work with them. But that doesn't happen. That is the frustration of the committee.

Mr. MICA. Mr. Chairman, if they continue just to—a point of procedure. I would be willing and I will advocate that we do subpoena the appropriate personnel. They send us people like this who cannot provide us with the information. This is the chief investigative committee of the U.S. House of Representatives. And they are going to appear one way or the other or cooperate one way or the other. And I put them on notice again today.

Mr. CHAFFETZ. I now recognize the gentleman from Texas, Mr. Farenthold, for 5 minutes.

Mr. FARENTHOLD. Thank you very much. I appreciate it. Sitting on committees that have the most jurisdiction over the TSA, I sit on this committee, Mr. Mica's Transportation and Infrastructure Committee, and the Homeland Security Committee. These are issues that deeply concern me in my work with Congress and I am happy you all are here. I'm happy to be able to discuss this again.

And I'm probably the recipient—I have gotten more TSA pat-downs since I have been in Congress than I have gotten pat-downs from my wife. Since the topic of this is perimeter security, I wanted to start with that, Mr. Sammon.

To what degree does the TSA coordinate with the FAA, for instance, on spending on airport security? I know in Corpus Christi we recently got about $5 million from the FAA to improve security. But has there been any action with the TSA in determining where the multiple dollars are best spent?

Mr. SAMMON. I think that is—since the GAO report you have seen come out, a number of things we have been working for several years to address the specific issue you're talking about. First of all, we worked with the airport community to come up with recommended design guidelines for airport planning and construction. A lot of the money the airports use for planning and construction comes from the FAA.

Next we worked with the Homeland Security Institute to develop a best practices from all of the airports.

Mr. FARENTHOLD. I'm sorry. I have a real short amount of time. But you are saying you're now working regularly with the other agencies to make sure the right hand knows what the left hand, the government, is doing?

Mr. SAMMON. What we are doing is working with the airports. They have a tool. It is a specific computer program they can run through their system. The idea is for the FSEs to work with the airports to come up with the optimal security spending per airport. It is not the same everywhere.

Mr. FARENTHOLD. Okay. And we talk about high-risk airports. What is not a high-risk airport when I can get on a commuter jet at any airport in the country and end up at a hub airport and be

on the biggest airliner in the world? What would not constitute a critical airport?

Mr. SAMMON. I agree with you 100 percent. The report we got in terms of the 700 innovative measures came from airports as small as Asheville, from the airports such as Delta County, Minot. So it is a mixture of big airports and small airports that have gotten into best practices in terms of what are the kinds of things that are appropriate for each airport.

Mr. FARENTHOLD. All right.

Again, let me go on to Mr. Orr. I apologize for jumping around. I have a lot of questions and a limited amount of time. You're talking about spending on, for instance, baggage screening equipment. I will just speak from experience. The airport I use most is the Corpus Christi Airport. We have 3 airlines, American and Continental with small regional jets, and Southwest with 737s. Each individual airline has a screening machine staffed by two TSA agents. We bought three machines for the Corpus Christi Airport and there is probably a fourth one because Delta used to come in there.

Why couldn't there just be one and a couple of TSA agents? There are never that many people there. Why are we—do we have any clue why we are spending multiple——

Mr. LORD. That is a great question. TSA has an electronic baggage screening program which they are trying to move to what they term "optimal solutions" for each airport. And essentially what that means is in many cases they are trying to remove the stand-alone machines and use more efficient systems or even so-called in-line systems, which require less personnel to operate. I'm not sure if that particular airport is on track to get an in-line system.

Mr. FARENTHOLD. All right.

And let me go to Mr. Ron for a second. One of the—one of the things I hear consistently from my constituents—try saying that three times fast—is why don't we follow more of the Israeli model of dealing with people instead of things? The answer I have gotten from a lot of people within our government is Israel only has a couple of airports and not nearly the amount of traffic that we have. Could we implement the Israeli system for a reasonable cost in the United States?

Mr. RON. Well, first I would like to say that the Israeli solution is not really an issue when it comes to volume. And I don't think that this is the main consideration. I think that the main consideration is that the Israeli legal culture, the environment is very different from the American one, and therefore I would not recommend to adopt the Israeli model as is.

But at the same time I strongly recommend that the concept that is driving the Israeli solution, which is identifying the level of risk of individual passengers and responding to them with a comparable level of search and an interview, as necessary, is the right way. And I think that an American solution that would be more comparable to the American environment can and should be developed and implemented.

Mr. FARENTHOLD. Thank you very much. I am out of time. I'm hopeful we will have a second round of questioning because I have at least 5 minutes more. Mr. Chairman, thank you.

Mr. CHAFFETZ. Thank you. I now recognize the gentleman from Arizona, Mr. Gosar, for 5 minutes.

Mr. GOSAR. Thank you. Inspector Parker, you know, we have spent—we have deployed 500 advanced imaging technology devices, spent $121—$122 million on the advanced imaging technology. We have also spent another $30 million on the puffer machines that shoot air blasts at passengers and sniff for explosives, but they rarely work properly.

Tell me what the end return on investment of dogs is. I mean, I see some problems with this, because you have to move everybody through these technologies, but that animal moves. It covers a wide range of ground. So tell me what the return on investment is.

Mr. PARKER. The return on it, sir, is mobility. You don't have to spend money to integrate any new odor to it because a dog is a little bit better than machinery, because technology—we can introduce odor that you come out anything new to a dog, and in 2 or 3 weeks they are proficient at it, as long as you keep that proficiency up.

Like I say, you can take the dog to an area, versus you have to bring people to an area, as you say. And it gives a lot of people more sense of security when they see a dog and especially when they can see a dog working. As you saw, the dog was standing there, people walk through. And we do it at Amtrak all the time. People come out on the Acela with that dog at the boarding gate and people are happy to see him and it is not intrusive and the dog is working. And who don't like dogs?

Mr. GOSAR. The person who doesn't like dogs I don't want to know. Tell me the average lifetime of an active K–9.

Mr. PARKER. Without any medical problems, we get a dog at a year old. I like to have the dog work until they are about 7 or 8 years old, because after the first 2 years or so, that is when the dog really gets into its prime again if he is well trained and proficient training is there. So you will get a good 5 years, without adding any software to him or getting a new breed because something else then came out. We just add it to a dog. We just add it to a scent pitcher and that is another odor that he is able to detect and perform.

Mr. GOSAR. You know, I'm a businessman, so tell me what the cost of that K–9 cost is.

Mr. PARKER. Well, it ain't the same cost as technology, sir.

Mr. GOSAR. Interesting. Would you say a little bit or a lot less?

Mr. PARKER. A lot less. And you have to understand dogs, like I say, don't depreciate. If anything, they go up more in value and they will be more effective when they get all of the training that they need.

Mr. GOSAR. Now, they are also very keen about detecting behavior, are they not?

Mr. PARKER. Yes, sir. And that is why the vapor wake dogs are very important right now, because they can screen people without them even being known. If you come to Amtrak, we do it all the time. And I know you know about the rush that comes through our gates. And these dogs screen people, and they keep on going without even being aware they are being searched.

Mr. GOSAR. Can they detect an implant, a bodily implanted device?

Mr. PARKER. Well, sir, scientifically right now, there is no data that says the dog can or cannot. But given the schematics of a person's body and, you know, dogs can detect cancer on people's bodies, tumors, the dogs can detect anything that they are taught. I think if the dog is taught to do that, he would be a very real good asset for that.

Mr. GOSAR. They are very innate about picking up differences in how people, as you said earlier. One of the biggest things, Mr. Sammon, I have seen in my limited time on the Hill is uncoordination of coordination. In fact, I had to put a bill just to break down jurisdictional boundaries of two different agencies. So it seems to me like the biggest problem that we have here is tell me who the lead is in all of this. Who is the kingpin? Who actually dictates how all surveillance or a perimeter security should be dictated?

Mr. SAMMON. As I said in my opening point, the airport—every airport has a plan. The airport is responsible for executing a plan with their people and——

Mr. GOSAR. I'm going to interrupt you again. Who is ultimately—that is not it. Is it Homeland Security? Who oversees the whole process of these whole aspects of a perimeter surveillance?

Mr. SAMMON. TSA oversees the plan and inspects the plan.

Mr. GOSAR. Okay. So you have the jurisdiction to do so?

Mr. SAMMON. We can—if there are deficiencies in the plan, we can levy fines of civil penalties, yes, sir.

Mr. GOSAR. So it seems to me that you could ante up all agencies to say, on a timely basis, that you do this. I mean, I have seen it. And just to give you a quick example, I have seen a flood, and I have seen an agency head from the Forest Service make sure that everybody is lined up in time, in real perspective, without delays. I have seen it happen. So I know it can happen. So it seems to me like the buck stops with you, then.

Mr. SAMMON. So, again, what we want to do—and I think one of the things that—with GAO, is a comprehensive look at what——

Mr. GOSAR. I'm very aware of what government does. It studies and studies and studies. And by the time you get a study out, it is antiquated. It seems like there should—wait a minute. It seems like there should be a minimum standard that is equating all the way across the board. And it seems like we are missing the point, because I think we need to be using Mr. Ron and Inspector Parker's ideas within this, because we have to have some minimal standards.

And I'm also from Arizona and so I know that those numbers are not right. I suspect that—well, just to give you a quick example. We are talking about those that you know about, security breaches. They are not the ones that you're not talking about, that you don't know anything about. And you can't tell me that those don't occur. We sit on the border and we are saying that we apprehend one in about every four.

I hope those aren't the same kind of numbers here. Because from what we have had in previous testimony, there is a lot of people carrying badges out there that we don't have any recollection of

and who they are and background. Seriously. That was brought up in this committee.

Mr. SAMMON. What you have is under about 850,000 people who have criminal history background checks and terrorist watch list checks in addition to other checks.

Mr. GOSAR. And it is inadequate. That is because—I can point to you that we take a grandmother and strip her down who is—because it must be the grimacing that she is going through terminal cancer—and that we also have another foreign national that gets through with an invalid visa. The problem is that there's problems with that aspect because we are not nimble enough and we are not working at associating with local and regional communities better. And that needs to stop. I'm out of time, sir.

Mr. CHAFFETZ. Mr. Sammon, if you wanted to——

Mr. SAMMON. No, no. I think—again, this effort—the tool which basically allows every airport, in conjunction with the Federal Security Director, to do that evaluation of what their vulnerabilities are, because they are unique, there isn't one standard that applies across the whole country. But you take those standards, apply them based upon the vulnerabilities, the attack scenarios that are possible at that airport, so on and so forth, for each airport to come up with an optimal solution so that every dollar that they have that they can apply to security, they do it in the optimal way, the best way, the best bang for the buck for that particular airport—that tool exists. It is done in collaboration with the airports and the airport authorities.

We had over 100 airports apply. Charlotte was not one of them. Charlotte is not particularly active in AAAE, which is a national organization which has security committees. They are not active in ACI, which is a national airport organization that has security committees. So of all of the people that worked on this, Charlotte's name is not in there. So there are people who are working on this.

As a matter of fact on Monday, I had the CEO of Dallas/Fort Worth Airport fly in with his senior staff to sit down with John Pistole and our group to tell us that they are very happy working with TSA, and what they wanted was to volunteer for any pilot security projects that they could have that we would work with them on.

So in terms of how the relationship with airports and working with local authorities, it may vary across the country, but there are a lot of them who put a lot of work into all of these reports to get a tool that will enable them to do the best, most optimal security assessments and reports and ways forward for each of the airports.

Mr. GOSAR. Well, then it seems to me that you just told me that you want a nimble approach. So maybe Charlotte needs a little different TLC and maybe that's what you need to look at, is that you're giving an individualized plan, so make sure that you're elevating that to an individualistic plan as well. You know, be careful what you ask for there. Okay?

Just because somebody is complying—to give you an example, you know, as a teacher, a teacher only is asking you to repeat what they want you to. It doesn't tell you about the knowledge about the student. You have to go a little bit further sometimes, and that is the exact case that I'm looking at is that sometimes the squeaky wheel is actually the one that is doing something a little bit dif-

ferent that I want to know about. And I think that behooves you at the top to understand what they are doing, why they are doing it, as well as all the different other models.

Mr. SAMMON. And that is why what we did is go beyond compliance with this report to get the best innovative security measures from airports around the country, because compliance is not sufficient.

Mr. CHAFFETZ. I agree. And we will probably have this ongoing discussion, but the idea that you haven't conducted joint vulnerability assessments in 83 percent of our Nation's airports is not acceptable. It is just not acceptable. We need to figure out how to solve that. And I appreciate the follow-up with that. As it relates to Dallas, I would hope that Dallas would be the first ones in here. They have had 20 perimeter security breaches in the last 5 years. They had a truck that actually came out across the field, as I noted in my opening statement. So there is a lot that needs to be done on security with such a big airport such as Dallas, for instance.

Let me go back to the dogs here. My understanding of the dollars and the metrics here,and, again, if we can correct the record here as a follow-up, my understanding is it costs roughly about $175,000 per whole body imaging machine, but the dogs are something like $20,000 to $30,000 to have a fully trained dog ready to go. Those aren't the numbers. Let us go ahead and correct the record. But I am pretty darn sure those are the records.

But to Mr. Gosar's point, the whole body imaging machines have something that the dogs don't have. They have lobbyists. And what is infuriating to a person like me is I think the challenge is we have to increase the security. We have to become more secure. But we can't give up every civil liberty. We shouldn't be looking at every passenger naked in order to secure the airplane. What we do need are these good dogs because the Pentagon, having spent $19 billion, came to the conclusion, as I pointed out with the lieutenant colonel's comments, the single best way to find a bomb-making device or bomb-making materials is the K–9. And we are not putting enough emphasis on expanding the use of K–9s. They are friendly. They are noninvasive. They are effective. They are the single best weapon, according to the Pentagon, in order to fight and find these explosive devices.

Mr. SAMMON. Would you like a response?

Mr. CHAFFETZ. Sure.

Mr. SAMMON. In terms of the dogs you saw here, the TSA supports the Amtrak program. In fact, we probably have supported up to about a third of the dog teams that Amtrak has. The dog—a fully equipped dog team with training, trainer, dog, so on and so forth, is in the hundreds of thousands of dollars because you don't—the dog doesn't—it does. You pay for the salary of the trainer——

Mr. CHAFFETZ. Per year?

Mr. SAMMON. Yes.

Mr. CHAFFETZ. You think that is per year? Hundreds of thousands of dollars? Hold up.

Inspector Parker, can you give me a sense of just—what does a dog handler make there at Amtrak? What is their annual salary? Do you have a guess of generally what they are making?

Mr. PARKER. It depends on their rank. They are probably at 50- to 70,000.

Mr. CHAFFETZ. So how do you come up with hundreds of thousands of dollars? I mean, Alpo only costs so much.

Mr. SAMMON. We oversee the Transit Grant Program where we provide dog teams to agencies around the country, and it is in excess of $100,000. We provide——

Mr. CHAFFETZ. You said hundreds of thousands of dollars per dog. I challenge you—I challenge you to verify that number.

Mr. SAMMON. We will get you the numbers that we——

Mr. FARENTHOLD. Will the gentleman yield?

Mr. CHAFFETZ. Yes.

Mr. FARENTHOLD. Will the gentleman yield for just 1 second?

Mr. CHAFFETZ. Sure.

Mr. FARENTHOLD. I assume that your whole body imaging machines require an operator, too, that requires a salary as well. They don't—it actually in Corpus Christi requires at least two, actually three, one to stop you going through, one to listen on the radio, and the one in the back that—it requires three operators for a whole body machine.

Mr. SAMMON. They all require—they are all expensive systems. They each have their role.

Mr. CHAFFETZ. You're suggesting that the whole body imaging machine is a cheaper alternative than using the K–9s. I tell you what, let's do this. I would love to do this. I would love to do this. You take 1,000 people and put them in a room, I will give you 10 whole body imagining machines. You give me 5,000 people in another room, you give me one of his dogs, and we will find that bomb before you find your bomb.

That is the problem. There is a better, smarter, safer way to do this. And the TSA is not prioritizing it. And if you look at who those lobbyists were that pushed through those machines, they should be ashamed of themselves, because there is a better way to do this and it is with the K–9s. And I'm basing that based on what the Pentagon did. That's what the Pentagon did. They studied all the technology, all the information; and that is what they are doing, they are deploying—you don't see whole body imagining machines in Kandahar, but you do see dog teams because those guys, their people—their lives are on the line every day. That's what we should be doing.

And you brought it up and I will challenge it. Let us go look at, dollar for dollar, what is more expensive, a whole body imaging machine, which we know is not effective, and a K–9. Let's see who can find more bombs and let's see who is less expensive. Let's move on.

Mr. SAMMON. And the dog does not work all day. Thank you.

Mr. CHAFFETZ. Inspector Parker, how long does the dog work?

Mr. SAMMON. The dogs will work 2 to 3 hours a day, sir. And you take a break, and they work 2 to 3 hours more is how you condition the dog to work.

Mr. CHAFFETZ. Let us keep going because I really do believe that the dogs are a better, smarter solution.

One of the challenges that the TSA is having to deal with is the fact that we have over 900,000 security badges out there. My un-

derstanding as I was told, there are roughly 16,000 just at Dulles Airport alone. What sort of background checks are they going through? How often are those rechecked? And how are you going to deal with the fact that we have closing in on a million people with security badges all across the airports?

Mr. SAMMON. There are probably 850,000 badges out there that are active. They go through a criminal history background check.

Mr. CHAFFETZ. Who does that check?

Mr. SAMMON. The—that check is—it goes through the airport authorities, AAAE to the FBI. Then they do a watch-list check, which goes through AAAEs, right. Currently the channeling mechanism goes through TSA. We run a watch-list check on them. They are perpetually vetted from the watch-list basis.

In addition, there are other immigration checks on those people versus when they originally apply. They are redone every 2 years. And at that time, the security awareness training is required at the time of the badge reissuance.

Mr. CHAFFETZ. Do you have a plan to deal with the vulnerabilities of an insider attack?

Mr. SAMMON. There are a number of things in terms of insider attacks, in terms of the security awareness training.

Mr. CHAFFETZ. No, but I'm saying is there an actual plan?

Mr. SAMMON. In terms of—what particular kind of attack?

Mr. CHAFFETZ. An insider attack.

Mr. SAMMON. Well, there are many—it can take many forms. What kind are you thinking of?

Mr. CHAFFETZ. I just wonder if there is a plan to deal with the fact that you have 900,000 people who are——

Mr. SAMMON. Yes.

Mr. CHAFFETZ. You do. Mr. Lord, what is your understanding of that situation?

Mr. LORD. Our commentary was related to the combined risk assessments, something called TSARA, the latest edition released last year. A notable caveat was it excluded the threat of the insider attack in various forms and TSA acknowledged it needed to look at that. And the next iteration due later this year will include that threat.

Mr. CHAFFETZ. But Mr. Sammon just said he already has it.

Mr. LORD. Well, I'm not sure he meant it in terms of this one analysis I'm referring to. They may look at it in other forms or——

Mr. CHAFFETZ. Is Mr. Lord wrong?

Mr. SAMMON. No. Two different things. Your question, as I took it, is what goes on daily in an airport environment. The TSARA is a—the first of its kind across all modes risk comparison, based upon 500—in excess of 550 attack scenarios. Insider attack was not part of the first one. It will be included in the second version.

Mr. CHAFFETZ. I look forward to seeing that. The 25,000 perimeter breaches, I would appreciate—is this—it is very difficult to get any sort of analysis of this over such a long period of time. Is there a month-by-month analysis that you can share with us?

Mr. SAMMON. I don't have it with me. That is 2,500 a year. It could be anything from a bag left behind, a door left open——

Mr. CHAFFETZ. That's where we are hoping that the TSA can provide us—introduce some details and understanding where the

trend is going. Is this an upward trend, downward trend? That sort of thing. Is that something that you will provide the committee?

Mr. SAMMON. I will go back and we will check into that, yes, sir.

Mr. CHAFFETZ. Yes, you will provide that to the committee?

Mr. SAMMON. In terms of—if it is security-sensitive material, we will talk to the committee about that, yes.

Mr. CHAFFETZ. All right.

Let me keep going. The perimeter fence at the JFK Airport, based on an investigative report done by a news organization, my understanding is that the project to fix the perimeter fence is running 4 years behind schedule. What is your knowledge of that situation?

Mr. SAMMON. I'm not personally aware of that. I do know that JFK and the New York Port Authority Airports are looking at deploying state-of-the-art intrusion detection technology in addition to fencing because of the kinds of things that people have talked about. The fence can be cut. You want to have a technology tied into camera systems that will alert cameras and patrols if there is an intrusion.

We deploy extensively in the subway tunnels, intrusion detection in key tunnels, and particularly underwater tunnels.

Mr. CHAFFETZ. I know. We are getting off topic here. I'm worried about the quarter mile of fence at JFK and it being 4 years behind schedule.

Mr. SAMMON. I don't know right now, today, what the status is, but we'll get back to you.

Mr. CHAFFETZ. Please describe for the committee your role and responsibility. What is your responsibility?

Mr. SAMMON. My responsibility is working with the various stakeholders, the various people in pipelines, in mass transit, in railroads, in highways, in air freight carriers generally——

Mr. CHAFFETZ. So it is not exclusive to just airports?

Mr. SAMMON. No, sir.

Mr. CHAFFETZ. And would you say that JFK is one of the most—I mean, it has to be one of the largest targets out there.

Mr. SAMMON. JFK is.

Mr. CHAFFETZ. The committee would appreciate more understanding from their perspective of why this project is 4 years behind schedule. I understand there is a local component. But from the TSA side, that would be much appreciated.

At Los Angeles International Airport, LAX, an airport official noted that although the current 8-mile perimeter fence complies with Federal regulations, that it has been built in stages of the past decade, it has no one consistent security standard. Is there a consistent security standard for perimeters?

Mr. SAMMON. The standard varies based upon the location of the facility——

Mr. CHAFFETZ. But it is not going to vary in an airport, right? It may vary between LAX and Bozeman, Montana.

Mr. SAMMON. It may vary based upon where the location of the airport is, what the surrounding geography is.

Mr. CHAFFETZ. Are there standards for all those various components?

Mr. SAMMON. Those standards are again—what we have done—the work I showed the committee earlier today in terms of developing what those—for each airport based upon their vulnerabilities. But they do vary with an airport. Some parts are——

Mr. CHAFFETZ. Mr. Lord, what is your understanding of this situation?

Mr. LORD. I will have to defer to Mr. Sammon on that, whether just standards vary within the actual airport. I don't have the expertise——

Mr. CHAFFETZ. In 2009, the Government Accountability Office issued a report stating that TSA lacks, "a unified national strategy." Where is that today?

Mr. LORD. Well, first of all, that is a great question. At the time we did the work, we were concerned about the variety of players involved—multiple layered ports, multiple industry stakeholders—TSA had more of an indirect oversight role. And we thought it was important to come up with an overall game plan to unify the current efforts. And it is our understanding that draft strategies currently have been included as a model annex to a document called the TSIP, but that is currently under agency review. So they are close to releasing it. We have not seen it yet.

Mr. CHAFFETZ. One more question and then I will recognize Mr. Farenthold.

The software updates. As Inspector Parker pointed out, the hardware needs software, and that software needs updating. Some of this software is as old as 1998, is my understanding based on what I have read. Is that your understanding? And what is the agency doing to update the software?

Mr. SAMMON. So as I understand the—all new equipment being purchased is being purchased at the 2010 standard, the 1998 standards are more stringent than anything in the world, and that there is a plan to update, incrementally, machines that are out there, in phases to the 2010 standard. That is my understanding.

Mr. CHAFFETZ. Mr. Lord, do you care to comment on that?

Mr. LORD. I agree with that characterization.

Mr. CHAFFETZ. So are you prioritizing the 1998 machines? Is there a——

Mr. SAMMON. I will have to get back to you with the specific plan to update those machines. I don't have that with me.

Mr. CHAFFETZ. All right. Let me go to Mr. Farenthold to be recognized.

Mr. FARENTHOLD. Thank you very much, Mr. Chairman. I appreciate the opportunity for a second round of questioning.

Again, I want to start with the actual topic that—we have kind of gone into a whole lot of areas here. Perimeter security. Once you are within the perimeter of the airport, there is a real potential of you being able to do some damage. What is being done to address much more ease of access to the tarmac area from those involved in general aviation as opposed to those in commercial aviation? For instance, I drive into the general aviation area to board my friend's private plane, and then I wander over and sneak something on a plane, a commercial plane.

Mr. SAMMON. The first thing we have done, about 2 years ago, required extending the badging requirements to people in general aviation. That caused quite a fuss. There was a lot of pushback on that.

Mr. FARENTHOLD. But now there's no photo IDs for a pilot to access his or her plane——

Mr. SAMMON. If he is regularly on that airport, he has to have a badge, yes, sir. If—based upon where it is. But if he has proximity to the tarmac, the commercial airport—and this caused quite a bit of ruckus I think back in 2008, when we extended the badging requirements for larger populations within the airport——

Mr. FARENTHOLD. But I don't need a badge to get onto the tarmac in a general aviation area. I don't need anything.

Mr. SAMMON. You either have to be accompanied to your aircraft back and forth or in and out of that facility. But if—you can be challenged, just as anyone else on the facility if you are there.

Mr. FARENTHOLD. All right. It seems like—again, I am just speaking from what appears to me to be common sense, that there really ought to be a focus on the ground staff that doesn't go up in the airplanes. The 9/11 box cutters were potentially put on the plane by ground crew. The ground crew doesn't go up with the plane, so their life isn't at risk in an attack. It seems like there ought to be a strong focus there.

Mr. SAMMON. That is why they are all badged, and they have security awareness training. That is why there is covert testing of those—and random screening of people on the tarmac, yes, sir.

Mr. FARENTHOLD. All right. And let us talk a little bit about the behavioral detection. You know, before I was elected to Congress, I actually had time to watch TV and watch Lie to Me. Is this really a science that works, or is it a pseudoscience? You mentioned that we were able to apprehend hundreds of criminals. Have we seen any positive results of that in apprehending anybody with contraband at the airport?

Mr. SAMMON. We did. I believe it was in Orlando several years ago, a person had actually explosive material in his bags. He attempted to get them onto the belt. He was detected as he came through the door by his behavior. He had not been screened. His bags had not been screened. He was pulled over and found that he had—was attempting——

Mr. FARENTHOLD. So we have gotten one. Mr. Lord, did you want to comment?

Mr. LORD. You know, I would like to respectfully disagree with Mr. Sammon on that. I'm not sure he was detected through the BDO program. He had such an unusual appearance, I think he alarmed the passengers waiting in line, and a ticket agent may have alerted locals. I'm not sure that was truly a BDO behavior detection success.

Also, as I recall from reading his case file, he is an Iraqi war veteran suffering from post-traumatic stress disorder and wasn't on his medication.

Mr. FARENTHOLD. Mr. Ron, would you like to comment on that? I know the Israelis were pioneers in this.

Mr. RON. Yes. The Israeli—the principle of behavior is part of a wider principle of identifying level of risk of the individual pas-

sengers, and it is also based on looking at other sources of information rather than just observation. So you have to look at it in that context.

But I still have to say that the BDO program, despite the fact that it has been noted that they—both by GAO and the Academy of Science, that there is no scientific support. But I need to say that there has not been serious research into this. So that by itself doesn't prove that it doesn't stand.

In empiric terms, I think that at least those airports here in the United States that we have worked with on this issue, mostly with local police officers, there has been a reasonable level of success in detecting people with malicious intentions.

Mr. FARENTHOLD. Let me just ask you one more question, Mr. Ron. If for some reason I were to become President tomorrow, and I appointed you the head of the TSA, what are the top five changes you would make to improve security and improve the efficiency of the system? Can you list maybe five off the top of your head?

Mr. RON. Well, I will start with two. The first one is a—I would redirect the strategy toward a risk-based—real risk-based strategy that identifies the level of risk of the individual passenger by the access to information that we have starting with, prior to his arrival, his or her arrival at the airport. And later on the—with the ability to talk to those very few passengers that we find as high-risk passengers based on our earlier analysis and not just search them, but also talk to them and interview them to a level that would provide us with more information.

Mr. FARENTHOLD. It is really interesting. I did this just kind of as a thought experiment and I will just give you—I walked—I went from Corpus Christi to Washington, DC, without saying anything other than thank you to a person at the airport. That was it. No interaction beyond saying thank you to people who helped me.

Mr. RON. This is a critical point because I think that the lack of contact between the security—between the security people and the passengers is one of our greatest shortcomings, because we just focus on items, and that is doomed to failure because the technology that we have at this point is not good enough to provide us with a reasonable level of detection.

Mr. CHAFFETZ. I now recognize Mr. Tierney.

Mr. TIERNEY. Thank you. Mr. Sammon, I just wanted to give you an opportunity to make some comments with respect to that.

Mr. SAMMON. Again, I don't disagree with what Mr. Ron is saying. The first thing in terms of what—the fundamental part is access to information; and that is the more information you have, the more you know about people and you can say—because most of the people going to the airport on any given day are all trusted. I mean, there is not—there is not a—they are fine. They just want to get on their way.

The challenge is to have information that differentiates people, one group of people or individuals from the larger group, and getting that, as he said, that information prior to their arrival at the airport. Right now we know, we know their name, we know their date of birth, and we know kind of where they are coming from and where they are going through. We can't, even through secure flight, track where they have been for the past 3 years. So it is—right

now we are in the situation of looking at how do we do better risk-based security, but also what kind of information can you have access to to do a better job? And that is one of the challenges.

Mr. CHAFFETZ. Thank you. Just some very quick things. The committee would appreciate the opportunity, particularly with Mr. Sammon here, to ask some additional questions. Would it be all right that we submit those. I would ask all Members of the panel—some of them weren't able to be here today—to submit those within the next 7 days.

We would also appreciate the TSA providing us a copy of each of the incident reports. I know it is a massive amount of paper, but we would like to pour through those. And we would appreciate it if you would provide those to us.

We would also like to have a briefing on this risk-based approach. It is something that you had offered earlier. I recognize that it probably needs to be in a secure setting, but it is something we would like to schedule and work out with the TSA, moving forward.

I would also appreciate some definitions, if you will, and some specific statistics on the number of stowaways. It is something that we have asked for. It is something that TSA has not yet provided to us but this committee would appreciate those.

Of those things that I asked, is there any reason to think that those things can't happen?

Mr. SAMMON. I will go back and check and make sure that they—the status of those requests and where they are.

Mr. CHAFFETZ. Thank you. And a couple of those are new. But the stowaways was a previous request.

The last question here about transportation security inspectors [TSIs], as it's referred to in a lot of the documents. How many of them are there? And I know that they can impose civil penalties. So how many civil penalties have we imposed over the years? I don't know what timeframe to ask, but——

Mr. SAMMON. I think that would be a good request in terms of what we have. I don't have data with me today, so it would merely be conjecture on my part. But we could give you the total number of inspectors that are out there and the number of penalties, the number of open cases. Also we do it in terms of findings. In some cases the airport, on the spot, resolves the issue. In other cases they do go to civil violations and civil fines and that kind of thing. But I think it would be good to get you a good breakout on that that is concise and accurate.

Mr. CHAFFETZ. We would appreciate that.

As we conclude here, I would like to give you just each a moment. Please, brief. But we'll start with you, Mr. Sammon, and kind of go down the line.

What is the kind of number one thing you would like to see happen, whether it is your biggest concern or what specifically you would like to see happen? And then we will close the hearing.

Mr. SAMMON. Again, with the committee and all committees in Congress, is to support and work with Administrator Pistole as he goes forward with the risk-based security. He is definitely focused in that direction. And it is going to take—there are going to be challenges as we referred to in terms of information: How do we

go forward? But he definitely is going in this direction. And I would say to give him the benefit of the doubt and work with him in terms of where he is trying to go.

Mr. LORD. I would just like to say on behalf of GAO, we stand ready to support the committee's efforts to oversee TSA's effort to move to more of risk-based approach. I agree with Mr. Ron; we need to spend more time worrying about dangerous people versus dangerous objects and there's various ways to do it. And we need to do it in a way that makes sense.

Mr. ORR. I would like to note that both of our joint vulnerability assessments noted no compliance issues. We were in full compliance with all of the regulations. What I would like to see is a collaborative partnership between us and the TSA to address the real issues.

Mr. CHAFFETZ. Thank you. Mr. Ron.

Mr. RON. Beyond the need for a better risk-based approach to passenger and bag screening, I would strongly recommend to create a better balance between the airport facility security and the passenger and bag screening operation, because right now we are spending most of our efforts on the front door when the back door is not secure at all.

Mr. CHAFFETZ. Thank you. Inspector Parker.

Mr. PARKER. Yes, sir. Thank you.

I would like to see continued support for the K–9 programs because, as I stated before, that Amtrak is doing a lot and we definitely appreciate what Congress has done for us to fund us.

Mr. CHAFFETZ. Thank you. Thank you all for being here. I appreciate it. It takes a lot of time and effort in preparation of your testimony and for you being here today. We do appreciate it. And thank you and I wish you the best.

Our mutual goal on both sides of the aisle is to make this country as safe and secure as possible, but at the same time we need to make sure that we are filling those gaps and asking the hard questions. That is what makes this country great, is our ability and opportunity to do that.

So, again, I appreciate you all being here. The committee stands adjourned.

[Whereupon, at 11:16 a.m., the subcommittee was adjourned.]

○