TEN YEARS AFTER 9/11: ASSESSING AIRPORT SECURITY AND PREVENTING A FUTURE TERRORIST ATTACK

FIELD HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT, INVESTIGATIONS, AND MANAGEMENT

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

SEPTEMBER 16, 2011

Serial No. 112–45

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

73–356 PDF WASHINGTON : 2012

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

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

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

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

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

SUBCOMMITTEE ON OVERSIGHT, INVESTIGATIONS, AND MANAGEMENT

MICHAEL T. MCCAUL, Texas, *Chairman*

GUS M. BILIRAKIS, Florida
BILLY LONG, Missouri, *Vice Chair*
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
PETER T. KING, New York *(Ex Officio)*

WILLIAM R. KEATING, Massachusetts
YVETTE D. CLARKE, New York
DANNY K. DAVIS, Illinois
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

DR. R. NICK PALARINO, *Staff Director*
DIANA BERGWIN, *Subcommittee Clerk*
TAMLA SCOTT, *Minority Subcommittee Director*

CONTENTS

Page

STATEMENTS

The Honorable Michael T. McCaul, a Representative in Congress From the State of Texas, and Chairman, Subcommittee on Oversight, Investigations, and Management:
Oral Statement 1
Prepared Statement 3
The Honorable William R. Keating, a Representative in Congress From the State of Massachusetts, and Ranking Member, Subcommittee on Oversight, Investigations, and Management 4

WITNESSES

Mr. Stephen M. Lord, Director, Homeland Security and Justice Issues, Government Accountability Office:
Oral Statement 7
Prepared Statement 9
Mr. Chris McLaughlin, Assistant Administrator for Security Operations, Transportation Security Administration, U.S. Department of Homeland Security:
Oral Statement 17
Joint Prepared Statement 18
Admiral George Naccara (Ret.), Federal Security Director, Transportation Security Administration, U.S. Department of Homeland Security:
Oral Statement 21
Joint Prepared Statement 18
Mr. Edward C. Freni, Director of Aviation, Massachusetts Port Authority:
Oral Statement 22
Prepared Statement 27
Major Michael P. Concannon, Major, State Police Troop F, Boston Logan International Airport:
Oral Statement 32
Prepared Statement 35

TEN YEARS AFTER 9/11: ASSESSING AIRPORT SECURITY AND PREVENTING A FUTURE TERRORIST ATTACK

Friday, September 16, 2011

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT, INVESTIGATIONS, AND MANAGEMENT,
COMMITTEE ON HOMELAND SECURITY,
Boston, MA.

The subcommittee met, pursuant to call, at 9:37 a.m., at the General Edward Lawrence Logan International Airport, Terminal E, Departure Level, Boston, Massachusetts, Hon. Michael T. McCaul [Chairman of the subcommittee] presiding.

Present: Representatives McCaul and Keating.

Mr. MCCAUL. Well, good morning to everybody here. The Committee on Homeland Security will come to order.

Let me first say thank you to the Massachusetts Port Authority and everybody involved with putting this hearing together. It's 10 years after 9/11. To be sitting in the very airport where the hijackers took off that fateful day is really something. I think it really brings a moment here as we reflect back 10 years later on aviation security.

Let me thank the Ranking Member for being such a great host. The Boston-Austin connection is still alive and well. I had the pleasure to bring him down to Texas, and it was about 110 degrees, so I really appreciate the 60-degree weather and sunny conditions. I think Mr. Keating is probably the envy of almost every Member in the House as he represents Martha's Vineyard, Nantucket, and Cape Cod. So I'm proud to represent Austin to Houston. Boston is not exactly a stranger to me. I did attend the Kennedy School at Harvard University many years ago.

So with that, we'll begin the hearing. The purpose of this hearing is to examine security at the Logan International Airport and aviation security throughout the United States 10 years after 9/11. This is an official House hearing, and so all of the rules of the House do apply to this hearing.

I now recognize myself for an opening statement. I know that sounds kind of strange, but that's how we talk in Washington. We have to recognize ourself to speak.

The morning of September 11, 2001, I remember watching the television with one of my daughters, and the first airplane had hit the Twin Tower and everybody thought it was an accident. Then the second plane hit, and she asked me, "Daddy, why did that

plane fly into the building?" It was when that second plane flew, at that point, we knew that this was not an accident. We knew that America was under attack.

There were a total of almost 3,000 deaths that day. It is estimated that the U.S. stock market lost $1.4 trillion in value. The United States was at war. We've lost thousands of men and women in the battle against terrorism, and we continue to fight the terrorists and protect our homeland.

The terrorists began this war by using our airports as launching pads. Over a period of 10 years, we've spent billions of dollars to mitigate such a threat. However, the 9/11 Commission's 10th anniversary report card concludes, "We are still vulnerable to aviation security threats." Specifically, the report states, "We need to improve screening at airport checkpoints using biometrics and standardized identification documents to make it more difficult to circumvent security."

In addition, the attempted terrorist bombing of Northwest flight 253 on approach to Detroit on Christmas day 2009 provides a vivid reminder that commercial aviation remains an attractive terrorist target and underscores the need for effective airport security. Our major airports now have multiple layers of security screening. Today's hearing will examine two of those layers, airport perimeter security as well as new security measures being tested here at Logan International Airport.

This airport has led the Nation in new techniques and innovative methods to prevent another 9/11 attack. Methods used by airports to control access vary because of differences in design and layout. But all access controls must meet minimum performance standards established by the TSA. TSA requires airports to control access using methods such as pedestrian and vehicle gates, keypad access codes with personal identification numbers, magnetic stripe cards and readers, turnstiles, locks and keys, and security personnel.

The Government Accountability Office's 2009 report concludes there have been thousands of security breaches at airports across this country.

Additionally, it's been reported a young man breached perimeter security at the Charlotte Douglas International Airport and hid in the wheel well of a passenger plane. His body was found along Boston's airport's flight path. Department of Homeland Security Secretary Napolitano said, "Clearly, if somebody, a 16-year-old, is able to circumvent standards and requirements and get into a wheel well of a plane, there has been a breakdown." Although some of these breaches are accidental, some may represent dry runs by terrorists.

The GAO examined airport perimeter security and concluded that the TSA should develop a comprehensive risk assessment of airport security and milestones for its completion and evaluation plan for any future airport security pilot programs and a National strategy for airport security that includes key characteristics such as goals and priorities.

Not only is perimeter security a special concern, but passenger screening is essential if we are to prevent another 9/11. TSA employees perform approximately 1.8 million screens per day, 2 million on holidays and have screened more than 6 billion travelers

since September 2001. The methodology has not always been perfect, and the sheer magnitude of this effort is certain to garner critics about the procedures.

TSA is attempting to improve security by testing a new program designed to identify potentially dangerous passengers before they board aircraft. The Screening Passengers by Observation Technique, or SPOT, originated right here at Boston Logan Airport in 2003. SPOT is designed to utilize nonintrusive behavior observation and analysis to identify high-risk passengers who may be a threat.

The Behavior Detection Program, a modification of SPOT, will have specially-trained agents question passengers, engage their reaction before they board the aircraft. Based on physical clues or answers to questions, these officers should be able to detect suspicious behavior. The analysis will help determine if a passenger should go through additional screening. The program is based, in part, on the Israeli model of passenger screening. The GAO has examined this program and concludes it should be fully validated before used in airports throughout the United States.

I hope I never have to answer a question for my daughter again about airplanes flying into buildings because of a terrorist attack. We are here today to make sure security is in place to prevent such questions and another tragedy.

Finally, I would like to, again, thank the Massachusetts Port Authority for hosting this hearing. You would never know that we're in an airport terminal here today. You've just done a fantastic job putting this together. I want to thank all of the witnesses for being here and everybody attending this hearing. Thank you for your interest and your participation.

[The statement of Mr. McCaul follows:]

PREPARED STATEMENT OF CHAIRMAN MICHAEL T. MCCAUL

The Committee on Homeland Security Subcommittee on Oversight, Investigations, and Management will come to order. The purpose of this hearing is to examine security at the General Edward Lawrence Logan International Airport.

I appreciate the effort taken on behalf of all of those involved to have this important field hearing. This is an official Congressional hearing, as opposed to a town hall meeting, and as such, we must abide by certain rules of the Committee on Homeland Security and of the House of Representatives. I kindly wish to remind our guests today that demonstrations from the audience, including applause and verbal outbursts, as well as the use of signs or placards, are a violation of the Rules of the House of Representatives. It is important that we respect the decorum and the rules of this committee. I have also been requested to state that photography and cameras are limited to accredited press only.

I now recognize myself for an opening statement. The morning of September 11, 2001, I remember watching television with one of my daughters and she asked "why did that plane fly into the building?" It was the second plane flying into the World Trade Center and at that point we knew it was no accident. America was under attack. There were a total of 2,996 deaths that day. It is estimated U.S. stocks lost $1.4 trillion in value. The United States went to war and we have lost thousands of men and women in the battle against terrorism. We continue to fight the terrorists and protect our homeland. The terrorists began this war by using our airports as launch pads. Over a period of 10 years we have spent billions of dollars to mitigate such a threat. However, the 9/11 Commission's tenth anniversary report card concludes "we are still vulnerable to aviation security threats." Specifically the report states we need to improve screening at airport checkpoints using biometrics and standardize identification documents to make it more difficult to circumvent security.

Additionally the attempted terrorist bombing of Northwest flight 253 on approach to Detroit on Christmas day 2009, provided a vivid reminder commercial aviation

remains an attractive terrorist target and underscores the need for effective airport security. Our major airports now have multiple layers of security.

Today's hearing will examine two of those layers; airport perimeter security, as well as new security measures being tested here at Logan International Airport in Boston. This airport has led the Nation in new techniques and innovative methods to prevent another 9/11 attack.

Methods used by airports to control access vary because of differences in the design and layout, but all access controls must meet minimum performance standards established by The Transportation Security Administration.

TSA requires airports to control access using methods such as pedestrian and vehicle gates, keypad access codes with personal identification numbers, magnetic stripe cards and readers, turnstiles, locks and keys, and security personnel. The Government Accountability Office 2009 report concludes there have been thousands of security breaches at airports around the country. Additionally, it has been reported a young man breached perimeter security at Charlotte/Douglas International Airport and hid in the wheel well of a passenger plane. His body was found along Boston airport's flight path. Department of Homeland Security Secretary Napolitano said, "Clearly if somebody, a 16-year-old, is able to circumvent standards and requirements and get into the wheel well of a plane, there has been a breakdown." Although some of these breaches are accidental, some may represent dry runs by terrorists.

The GAO examined airport perimeter security and concluded that TSA should develop a comprehensive risk assessment of airport security, and milestones for its completion; an evaluation plan for any future airport security pilot programs; and a National strategy for airport security that includes key characteristics, such as goals and priorities. Not only is perimeter security of special concern, but passenger screening is essential if we are to prevent another 9/11. TSA employees perform approximately 1.8 million screens a day, 2 million on holidays and have screened more than 6 billion travelers since September 2001. The methodology has not always been perfect. The sheer magnitude of this effort is certain to garner critics about the procedures. TSA is attempting to improve security by testing a new program designed to identify potentially dangerous passengers before they board aircraft. The Screening Passengers by Observation Technique (SPOT) originated at Boston Logan airport in 2003. SPOT is designed to utilize non-intrusive behavior observation and analysis to identify high-risk passengers who may be a threat.

The Behavior Detection Program, a modification of SPOT, will have specially-trained agents question passengers and gauge their reaction before they board aircraft. Based on physical clues or answers to questions, these officers should be able to detect suspicious behavior. The analysis will help determine if a passenger should go through additional screening.

The program is based in part on the Israeli model of passenger screening. The GAO has examined this program and concludes it should be fully validated before it is used in airports throughout the United States.

I hope I never have to answer a question from my daughter again about planes flying into a building because of a terrorist attack. We are here today to make sure security is in place to prevent such questions and another tragedy.

One final note; I would like to thank the Massachusetts Port Authority for hosting this hearing, all the witnesses present and especially my friend and colleague, Congressman Bill Keating for his insights about aviation security. With that I recognize the Ranking Member of the subcommittee, the gentleman from Massachusetts, Mr. Keating, for 5 minutes for the purpose of making an opening statement.

Mr. MCCAUL. With that, I would like to recognize my good friend and colleague, the Ranking Member of the committee, Bill Keating.

Mr. KEATING. Thank you, Mr. Chairman.

Now, last Sunday was a somber reminder of our lives, all of our lives, and the way that the tranquility that we had prior to that had been lost and lost forever, frankly. In the midst of our remembrance, there is still a great deal of struggle to comprehend exactly what led to the tragedy and how it could have been prevented.

The fact of the matter is that, on September 11, 2001, our aviation security suffered a profound breach. This breach resulted in over 3,000 lives lost and a new understanding of what it means to be safe. We are living in a world where the reality has changed,

and we know now that harm can strike at any moment on our own soil.

Thereafter, many things have occurred. I think it's fitting and appropriate that the Committee on Homeland Security is here today at Logan Airport to examine the strides we've made in our aviation security since the terrible day of 9/11 and the steps we need to continue to take to ensure that we remain ahead of those who desire to attack us.

I'd like to thank the MassPort Authority for their hospitality and their work in preparation for this hearing. I want to welcome two Michael McCauls. First, if I could, young Michael McCaul is here, 10 years old, and we welcome him to Boston. I also want to welcome Chairman Michael McCaul to Massachusetts. I'm happy to say that you're looking at two people who generally support the spirit of bipartisanship. Chairman McCaul's support was instrumental in conducting this hearing, and I thank him for that.

Last month, I had the pleasure to travel to Houston to conduct a field hearing in Chairman McCaul's home State where we examined security procedures at the Port of Houston. Mr. Chairman, just as the lessons we learned at that hearing at the Port of Houston allowed me to better understand and address the issues of concern at the Port of Boston, I hope the procedures and pilot programs we'll examine here today at Logan Airport can one day be applied to airports Nation-wide.

After all, Logan has become the gold standard for airports across the United States. The cooperation, security protocol, and technology employed here are impressive in every respect. Yet Logan's path to success originated in a place of sorrow when, a decade ago, terrorists chose this airport as one of their departure points in their quest to commit the most heinous terrorist attack to occur on U.S. soil. The devastating events of that day forever changed our Nation, and our security procedures have to adapt and change as well.

On September 12, 2001, the leadership at Logan was faced with a choice, to remain frozen in time or to move forward and establish the reputation as one of the safest and most secure airports in the United States of America. To the benefit of all those who travel in and out of Logan, like I do each week, I'm pleased to say, they chose the latter.

To date, Logan is the only airport in the country that conducts a daily security briefing that includes Federal, State, local law enforcement agencies, TSA, airport personnel, airlines, and MassPort staff. I had the opportunity to observe one of those briefings last June, and the high level of communication and cooperation that occurs here is truly outstanding.

This type of intelligence sharing should be routine. Yet as we recently saw in the 9/11 Commission's latest report, it's one of the areas where our homeland security continues to lack efforts. I hope we learn today how you conduct it here, even weekends, 7 days a week, and how important that is, and hopefully, that can be a message that goes to every airport across the United States of America.

Three weeks ago, Logan is the only airport in the country instituting an on-site Joint Terrorism Task Force. Furthermore, by December 31, 2002, Logan was the first and only major U.S. airport

to meet the Federally-mandated deadline to have 100 percent in-line baggage screening for passengers. Today, as most people here heard, they're announcing the second generation of that kind of screening.

In August 2006, the Massachusetts State Police started roadblocks to conduct random vehicle searches entering the airport premises. In March 2011, it became the first U.S. airport to fully implement full-body scanners. At least 1,000 new cameras are in place, including a pilot for a state-of-the-art 360-degree camera system that will improve video surveillance by leaps and bounds. These changes are laudable and should serve as the best practices Nation-wide.

But through my time as Norfolk District Attorney and now in my capacity as Congressman for Massachusetts and a Ranking Member in this Homeland Security subcommittee, I'm particularly concerned about the lack of Nation-wide standards of perimeter security. That addresses fences, barriers, areas that surround airports.

According to the GAO, in their 2009 report on the TSA, TSA hadn't conducted vulnerability assessments for 87 percent of the Nation's 450 commercial airports, nor has it developed a Nationwide strategy that fully addresses perimeter security. The lack of adequate perimeter security could, in one of the worst-case scenarios, result in individuals with nefarious purposes accessing secure airport areas by simply climbing over a fence, and in some cases, overcoming even less of a barrier.

This region has witnessed first-hand the devastating results that inadequate airport fencing can lead. In November 2010, the body of a 16-year-old tragically was found in Milton, Mass., Delvonte Tisdale from North Carolina. As a District Attorney, I was given the opportunity and the challenge to investigate that. Mr. Tisdale's case remains on-going. But investigators found that he breached the perimeter of a Charlotte Douglas Airport, gained access to an aircraft by climbing into and stowing away in the wheel well of a commercial airline and subsequently fell to his death as the aircraft made its final approach into Boston. Unfortunately, this is not an isolated incident.

We hope today to learn what strides you've made here. We hope to share that knowledge Nation-wide. I truly thank all of you for taking the time to be with us this morning. Thank you, Mr. Chairman. I'll yield my time back.

Mr. MCCAUL. I thank the Ranking Member, Mr. Keating. With that, I'm going to introduce the witnesses and look forward to hearing their testimony.

First, we have Mr. Stephen Lord. He is the Director of Homeland Security and Justice Issues at the Government Accountability Office. He is responsible for overseeing and directing the GAO's various engagements on issues related to aviation and service transportation. In addition to holding a bachelor's degree from the University of Virginia, Mr. Lord holds an MBA from George Mason University and an M.S. in national security strategy from the National War College.

Thank you, Mr. Lord, for being here today.

Next, Mr. Chris McLaughlin. He is the Assistant Administrator for Security Operations at TSA at the U.S. Department of Home-

land Security. He has over 10 years' experience in airport security, leadership, and operations management, as well as extensive experience in managing multimillion-dollar projects, developing operational plans and strategies, and improving operational and personnel performance. Mr. McLaughlin holds a B.A. from Connecticut College, where he graduated magna cum laude.

Next we have Admiral George Naccara. He is the Federal Security Director for TSA at the Department of Homeland Security. Prior to his work at TSA, the Admiral served 33 years in the United States Coast Guard.

Thank you for your service, Admiral.

He holds a bachelor's degree from the U.S. Coast Guard Academy and a master's degree from Central Michigan University.

Thank you for being here.

Next, Mr. Edward Freni—am I pronouncing that right?

Mr. FRENI. Yes.

Mr. MCCAUL. I apologize.

He is director of aviation at the Massachusetts Port Authority. Mr. Freni has over 30 years of executive experience with Logan International Airport and American Airlines. Mr. Freni holds a bachelor of science degree from the Whittemore School of Business.

Thank you so much for being here, and thanks for all you've done to make this airport safer.

Major Michael Concannon is a 26-year veteran of the Massachusetts State Police. He currently serves as the commanding officer of Troop F at Boston Logan International Airport. In this capacity, he also serves as the director of aviation security for the Massachusetts Port Authority. He is a 1987 cum laude graduate of the University of Massachusetts at Lowell and a 1996 cum laude graduate of Suffolk University Law School. He was admitted to the Massachusetts Bar in December 1996.

So I want to thank all of you for being here today.

With that, I recognize our first witness, Mr. Lord.

STATEMENT OF STEPHEN M. LORD, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. LORD. Chairman McCaul, Ranking Member Keating, thanks for inviting me here today to discuss aviation security issues.

The first thing I'd like to note is, security and commercial aviation operations is difficult given the hundreds of airports, thousands of daily flights and millions of passengers streaming through airport checkpoints on a daily basis. I'd also like to note that TSA spends several billion dollars each year in this endeavor.

Today, I'd like to discuss 2 of the 20 layers of aviation security. The first is, as you mentioned previously, TSA's Behavior Detection Program, also called SPOT. I'd also like to discuss various airport perimeter security issues.

First, regarding TSA's Behavior Detection Program, we issued a major report on this program in May 2010. The bottom line of our report is, while DHS has made an effort to validate the science underlying the program, more actions are needed. Additional steps need to be taken to ensure its full validity.

As we noted in the report, TSA deployed the program on a Nation-wide basis before first determining there was a valid scientific basis for the program. Earlier this year, April 2011, DHS completed an initial validation study. But the study itself made several important recommendations, additional actions that need to be taken to ensure it had a sound scientific basis. That was a positive step. But again, additional work is going to be needed to be taken to ensure its validity.

Some of the recommendations made in this report mirrored the recommendations we made in our big report, such as doing a cost-benefit analysis to help guide its deployment.

I'd also like to briefly highlight another important recommendation we made in our SPOT report, and that was to empower the Behavior Detection Officers to better link them to the intel databases that TSA has at its disposal. We thought those links could be improved, because we think it's really important to fuse the screening personnel with the intel process, sort of to help better connect the dots. As Representative McCaul mentioned, that was an important 9/11 Commission Act recommendation.

In sum, while TSA has taken actions to address our report recommendations, additional steps are still going to need to be taken to ensure you can apply these behavior detection principles on large-scale in the airport environment.

I'd now like to discuss some of the findings from our 2009 Report on Airport Perimeter Security. Now, first of all, I think it's important to recognize, TSA undertakes a whole host of activities to help secure airport perimeters and maintain effective access controls. They do random worker screening. They've expanded the requirements for name-based background checks. They're encouraging industry to adopt biometric security standards. However, at the time of our report, TSA had not completed a comprehensive risk assessment of airports. It's important to do a risk assessment, because that really helps you decide where to focus your resources.

The risk assessment also that they did complete in July 2010 did not fully consider the potential vulnerabilities of a so-called insider attack, which TSA views as a significant threat. The good news is that the risk of an insider attack will be included in the next update TSA is doing later this year, which is due later this year.

We also recommended that TSA consider making greater use of the so-called joint vulnerability assessments to identify airport vulnerabilities, and these are really an important tool in the TSA toolbox. In fact, we consider them the gold standard because they're rigorous, they're documented and they're completed with the FBI. The latest data shows, they've completed these at 17 percent of the Nation's airports.

Again, just to clarify, we're not recommending that you need to do them for 100 percent of the airports, but we think it's an important tool that they could more effectively apply on a larger scale.

Also one positive development I'd like to reflect is that they've recently developed a new tool to help assess airport vulnerabilities. It's called the Airport Security Self-Evaluation Tool, or ASSET, and this thing is just being rolled out. So I think over time, as they apply this to airports such as Boston, it will help Federal Security

Directors, such as Mr. Naccara, to help get a better sense of where to focus their protective efforts.

Mr. Chairman, Mr. Keating, this concludes my statement, and I look forward to answering any questions that you have. Thank you.

[The statement of Mr. Lord follows:]

PREPARED STATEMENT OF STEPHEN M. LORD

SEPTEMBER 16, 2011

GAO HIGHLIGHTS

Highlights of GAO–11–938T, a testimony before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, 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 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. Two 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; and (2) airport perimeter and access controls security. This testimony provides information on the extent to which TSA has taken actions to validate the scientific basis of SPOT and strengthen airport perimeter security. This statement is based on prior products GAO issued from September 2009 through September 2011 and selected updates in August and September 2011. To conduct the updates, 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 and airport perimeter and access control security efforts. DHS and TSA generally concurred with the recommendations and have actions under way to address them.

AVIATION SECURITY: TSA HAS MADE PROGRESS, BUT ADDITIONAL EFFORTS ARE NEEDED TO IMPROVE SECURITY

What GAO Found

DHS completed an initial study in April 2011 to validate the scientific basis of the SPOT program; however, additional work remains to fully validate the program. In May 2010, GAO reported 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. TSA is pilot testing revised program procedures at Boston-Logan airport in which behavior detection officers will engage passengers entering screening in casual conversation to help determine suspicious behaviors. TSA plans to expand this pilot program in the fall of 2011. GAO recommended in May 2010 that DHS, as part of its validation study, assess the methodology to help ensure the validity of the SPOT program. DHS concurred and stated that the study included an independent review with a broad range of agencies and experts. The study found that SPOT was more effective than random screening to varying degrees. 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 also noted that additional work was needed to comprehensively validate the program. TSA officials are assessing the actions needed to address the study's recommendations but do not have time frames for completing this work.

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 had 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 for security by TSA in 2009. GAO recommended that TSA develop: (1) A comprehensive risk assessment and evaluate the need to conduct airport vulnerability assessments Nation-wide, and (2) a National strategy to guide efforts to strengthen airport security. DHS concurred and TSA stated that the Transportation Sector Security Risk Assessment, issued in July 2010, was to provide a comprehensive risk assessment of airport security. However, this assessment did not consider the potential vulnerabilities of airports to an insider attack—an attack from an airport worker with authorized access to secure areas. In August 2011, TSA reported that transportation security inspectors conduct vulnerability assessments annually at all commercial airports, including an evaluation of perimeter security. GAO has not yet assessed the extent to which inspectors consistently conduct vulnerability assessments. TSA also updated the Transportation Systems—Sector-Specific Plan, which summarizes airport security program activities. However, the extent to which these activities were guided by measurable goals and priorities, among other things, was not clear. Providing such additional information would better address GAO's recommendation.

Chairman McCaul, Ranking Member Keating, and Members of the subcommittee: I appreciate the opportunity to participate in today's hearing at Boston-Logan International Airport to discuss two key layers of aviation security: The Transportation Security Administration's (TSA) behavior-based passenger screening program and airport perimeter and access controls.[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 the ability to detect, disrupt, and defeat plots to attack the homeland.[2]

Securing commercial aviation operations remains 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. For fiscal year 2011, TSA had about 54,800 personnel and its budget authority was about $7.7 billion. However, risks to the aviation system remain. Earlier this month, we reported on the progress made in securing the aviation system in the 10 years since the September 11, 2001, attacks and the work that still remains.[3]

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.[4] Criminal incidents involving airport workers using their access privileges to smuggle weapons and drugs into secure areas and onto planes have heightened concerns about the risks posed by workers and the security of airport perimeters and access to secured 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), and (2) strengthen the security of airport perimeters and access controls.

This statement is based on our prior products issued from September 2009 through September 2011, and includes selected updates conducted in August and September 2011 on TSA's efforts to implement our prior recommendations regarding SPOT and airport perimeters and access to secure areas of airports.[5] For our May

---

[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, DC: June 28, 2011).

[3] See GAO, *Department of Homeland Security: Progress Made and Work Remaining In Implementing Homeland Security Missions 10 Years After 9/11,* GAO–11–881 (Washington, DC: Sept. 7, 2011).

[4] 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.

[5] 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,

2010 report on SPOT, we reviewed relevant literature on behavior analysis by subject matter experts.[6] We conducted field site visits to 15 TSA-regulated airports with SPOT to observe operations and meet with key program personnel.[7] 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, 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.[8] For the updates, we analyzed documentation from TSA on actions it has taken to implement recommendations from our 2009 report, including efforts to conduct a comprehensive risk assessment and evaluate the need to conduct an assessment of security vulnerabilities at airports Nationwide, and to develop a National strategy for airport perimeters and access controls security that identifies key elements such as goals and priorities. As part of our efforts to update this information, we analyzed TSA data on the number of vulnerability assessments conducted at airports from fiscal year 2004 through July 1, 2011, by airport. More detailed information on our scope and methodology can be found in our prior reports.

All of our work was conducted in accordance with generally accepted Government auditing standards.

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 United States, 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 (BDO), who examine passenger behaviors and appearances to identify passengers who might pose a potential security risk at TSA-regulated airports;[11] TSA

DC: Sept. 30, 2009); *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, DC: May 20, 2010); *Aviation Security: TSA Has Taken Actions to Improve Security, but Additional Efforts Remain,* GAO–11–807T (Washington, DC: Jul. 13, 2011); and GAO–11–881.

[6] National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment* (Washington, DC: 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.

[7] 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.

[8] See GAO–09–399.

[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.

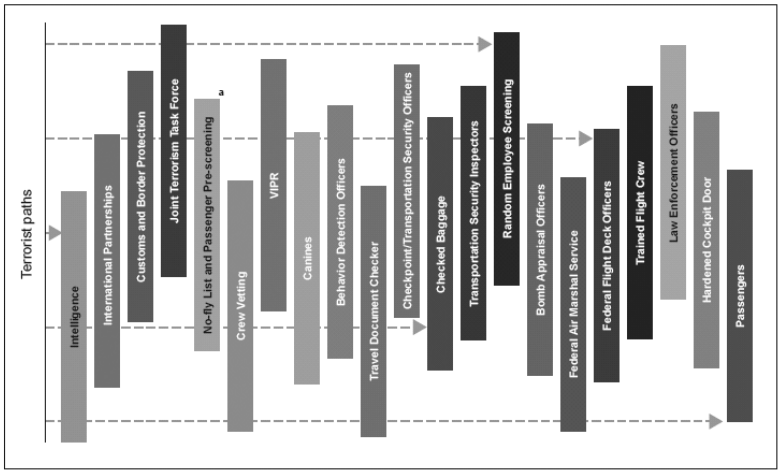
[10] Private-sector screeners under contract to and overseen by TSA, and not TSOs, perform screening activities at airports participating in TSA's Screening Partnership Program. See 49 U.S.C. § 44920. According to TSA, 16 airports participated in the program as of July 2011.

[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

Continued

has selectively deployed about 3,000 BDOs to 161 of 463 TSA-regulated airports in the United States, including Boston-Logan airport where the program was initially deployed in 2003. Other security layers include 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] Additional layers cited by TSA include, among others, intelligence gathering and analysis; passenger prescreening against terrorist watch lists; 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.[13] 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.[14] 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.

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 pre-empted, deterred, or to fail during the attempt.

---

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.

[13] Working alongside local security and law enforcement officials, VIPR teams conduct a variety of security tactics to introduce unpredictability and deter potential terrorist actions, including random high-visibility patrols at mass transit and passenger rail stations and conducting passenger and baggage screening operations using specially trained behavior detection officers and a varying combination of explosive detection canine teams and explosives detection technology.

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

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 Nation-wide 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.[15] 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.[16] 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, additional work 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.[17] 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 arrested for other reasons. As noted in our May 2010 report, SPOT officials told us that it is not known if the SPOT program has resulted in the arrest of anyone who is a terrorist, or who was planning to engage in terrorist-related activity. According to TSA, in fiscal year 2010, SPOT referred about 50,000 passengers for additional screening and about 3,600 referrals to law enforcement officers. The referrals to law enforcement officers yielded approximately 300 arrests. Of these 300 arrests, TSA stated that 27 percent were illegal aliens, 17 percent were drug-related, 14 percent were related to fraudulent documents, 12 percent were related to outstanding warrants, and 30 percent were related to other offenses. DHS has requested about $254 million for 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.

According to TSA, as of August 2011, TSA is pilot testing revised procedures for BDOs at Boston-Logan airport to engage passengers entering screening in casual conversation to help determine suspicious behaviors. According to TSA, after a passenger's travel documents are verified, a BDO will briefly engage each passenger in conversation. If more information is needed to help determine suspicious behaviors, the officer will refer the passenger to a second BDO for a more thorough conversation to determine if additional screening is needed. TSA noted that these BDOs have received additional training in interviewing methods. TSA plans to expand this pilot program to additional airports in the fall of 2011.

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.[18] 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.[19] According to the report, a terrorist's desire to avoid detection makes information-gathering techniques, such as asking what a person has done, is doing, or plans to do,

[15] See GAO–10–763.

[16] See DHS, *SPOT Referral Report Validation Study Final Report Volume I: Technical Report* (Washington, DC: 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.

[17] See GAO–10–763.

[18] 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.

[19] 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.

highly unreliable. Using these techniques to elicit information could also have definite privacy implications. These findings, in particular, may be important as TSA moves forward with its pilot program to expand BDOs' use of conversation and interviews with all passengers entering screening.

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 was 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.[20] DHS concurred and 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.[21] 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.[22] 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. In another example, BDOs could not input all behaviors observed in the SPOT database because the database limited entry to eight behaviors, six signs of deception, and four types of prohibited items per passenger referred for additional screening. Because of these data-related issues, we reported that meaningful analyses could not be conducted at that time 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 for this study used SPOT data recorded prior to these additional controls being implemented.

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.[23] Some of these recommendations, such as the need for a comprehensive program evaluation including a cost-benefit analysis, reiterate recommendations made in our May 2010 report. TSA is currently reviewing the study's findings and assessing the

---

[20] See GAO–10–763.

[21] 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.

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

[23] 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.

steps needed to address DHS's recommendations but does not have time frames for completing this work. 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 the broad scope of the additional work and related resources identified by DHS for addressing the recommendations. Thus, as we reported in March 2011, Congress may wish to consider the study's results in making future funding decisions regarding the program.[24]

TSA HAS TAKEN ACTIONS TO STRENGTHEN AIRPORT PERIMETER AND ACCESS CONTROLS SECURITY, BUT ISSUES REMAIN

We reported in September 2009 that TSA has implemented a variety of programs and actions since 2004 to improve and strengthen airport perimeter and access controls security, including strengthening worker screening and improving access control technology.[25] For example, to better address the risks posed by airport workers, in 2007 TSA implemented a random worker screening program that was 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).[26] 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.[27] 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 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 Nation-wide.[28] 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.[29] Our analysis of TSA data showed that from fis-

---

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

[25] GAO–09–399.

[26] GAO–09–399. DHS developed the NIPP to guide risk assessment efforts and the protection of the Nation's critical infrastructure, including airports.

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

[28] GAO–09–399.

[29] 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 air-

Continued

cal 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.[30] 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. 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 Nation-wide. 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 2009 report recommendation to assess the need for a vulnerability assessment of airports Nation-wide, and TSA officials stated that based on our review they intended to increase the number of JVAs conducted at Category II, III, and IV airports and use the resulting data to assist 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.[31]

Since we issued our report in September 2009, TSA had not conducted JVAs at Category III and IV airports.[32] TSA stated that the TSSRA is to provide a comprehensive risk assessment of airport security, but could not tell us to what extent it has studied the need to conduct JVAs of security vulnerabilities at airports Nation-wide. Additionally, in August 2011 TSA reported that its National inspection program requires that transportation security inspectors conduct vulnerability assessments at all commercial airports, which are based on the joint vulnerability assessment model. According to TSA, every commercial airport in the United States receives a security assessment each year, including an evaluation of perimeter security and access controls. We have not yet assessed the extent to which transportation security inspectors consistently conduct vulnerability assessments based on the joint vulnerability model. Providing additional information on how and to what extent such security assessments have been performed would more fully address our recommendation.

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.[33] 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 the summer of 2010.[34] TSA provided a

---

ports 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 every 3 years, or more frequently, as necessary, at each airport determined to be high-risk). Pursuant to ATSA, responsibility for conducting JVAs transferred from FAA to TSA. For more information on this issue, see GAO–09–399.

[30] 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.

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

[32] 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 6 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.

[33] GAO–09–399.

[34] 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.

copy of the updated plan to Congressional committees in June 2011 and to us in August 2011. We reviewed this plan and its accompanying aviation model annex and found that while the plan provided a high-level summary of program activities for addressing airport security such as the screening of workers, the extent to which these efforts would be guided by measurable goals and priorities, among other things, was not clear. Providing such additional information would better address the intent of our recommendation.

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

Mr. MCCAUL. Thank you, again, Mr. Lord.

The Chairman now recognizes Mr. McLaughlin for his testimony.

STATEMENT OF CHRIS MC LAUGHLIN, ASSISTANT ADMINISTRATOR FOR SECURITY OPERATIONS, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. MCLAUGHLIN. Good morning, Chairman McCaul and Ranking Member Keating. I'm pleased to appear before you today to discuss aspects of the Transportation Security Administration's security operations at U.S. commercial airports. I will restrict my comments to broader TSA policies and objectives while Federal Security Director Naccara will address issues and initiatives specific to Boston Logan International Airport.

As you know, the Aviation and Transportation Security Act, or ATSA, authorized TSA to work with U.S. airports and operators to strengthen security at access and critical control points throughout the United States. While TSA's aviation security standards provide a foundation for a comprehensive National program, the distinctive footprint, location, and requirements of each airport require each facility to have its own airport security program.

TSA secures commercial airports through a variety of programs. The programs most familiar to the traveling public include passenger screening operations conducted by Transportation Security Officers at security checkpoints, carry-on and checked baggage screening, and the Secure Flight Program which fulfills a key 9/11 Commission recommendation to implement a uniform watchlist matching program for all passengers traveling from, within, or bound for United States against names on Government terrorist watch lists.

Other layers of security play an equally important role and focus on preventing and detecting the unauthorized entry, presence, and movement of individuals and ground vehicles into and within the secured and airport operations areas of an airport. TSA maintains random and unpredictable security measures that may be employed at direct access points and airport perimeters, including vehicle inspections, explosive trace detection, enhanced screening, accessible property searches, as well as behavior detection.

As required by statute, TSA proscribes procedures for screening individuals, inspecting goods, property, vehicles, and other equipment before entering into the secure area of an airport. These procedures safeguard against unauthorized persons having access to aircraft, thereby reducing opportunities for criminal behavior. These safeguards also help ensure the safety and integrity of other individuals involved in aviation, including aircraft service providers and workers involved in catering and passenger amenities on-board

aircraft. Like-wise, TSA requires security access programs for vendors with direct access to airfields and aircraft.

Ultimately, the airport authority is responsible for abiding by the perimeter security regulations set by TSA and must establish procedures for its personnel and resources. TSA also conducts airport inspections to enhance security and mitigate risk associated with perimeter security. These include joint vulnerability assessments as well as regulatory special emphasis inspections that focus on specific aspects of the operation and the testing of airport access control processes. Based upon the results of these inspections and assessments, TSA develops mitigation strategies to enhance an airport's security posture and determine if any changes are required.

To counter the potential risk to perimeter security, TSA also deploys Transportation Security Inspectors to help determine whether airport operators are complying with TSA regulations and the airport's ASP. TSIs focus their assessments on security throughout the airport environments ranging from the curbside of the airport to the outermost perimeter fences. TSIs can recommend that civil penalties be assessed by TSA when repeated or egregious instances of noncompliance of regulations and security procedures are discovered.

Earlier this year, TSA initiated a special emphasis assessment and a special emphasis inspection of all Category X and I through IV airports evaluating perimeter security, including fencing, nonfence, manmade barriers, natural barriers, CCTV, electronic intrusion and motion detection devices and other barriers. Assessments are complete at all Cat X and I airports and the remaining airport assessments are expected to be completed later this month.

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.

I want to thank the subcommittee for this opportunity to speak to you today and discuss these important issues, and I'm happy to answer any questions that you might have.

[The joint prepared statement of Mr. McLaughlin and Admiral Naccara follows:]

JOINT PREPARED STATEMENT OF CHRISTOPHER MCLAUGHLIN AND GEORGE NACCARA

SEPTEMBER 16, 2011

Good morning, Chairman McCaul, Ranking Member Keating, and distinguished Members of the subcommittee. We are pleased to appear before you today to discuss the Transportation Security Administration's (TSA) security operations at U.S. commercial airports and to address any questions you may have about security at Logan International Airport (BOS) in particular.

As you know, the Aviation and Transportation Security Act (ATSA), (Pub. L. 107–71), authorized TSA to work with U.S. airport operators to strengthen security at access and critical control points throughout the United States to maximize the security of passengers and aircraft.

While TSA's aviation security standards provide a foundation for a comprehensive National aviation security program, the distinctive footprint, location, and requirements of each airport require each facility to have its own Airport Security Program (ASP). The ASP at Logan Airport 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 that may be unique to Logan.

TSA'S PRIMARY MISSION: 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 (TSOs) at security checkpoints; carry-on and checked baggage 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 United States against names on Government terrorist watch lists. Other layers of security play an equally important role in safeguarding our Nation against terrorist threats. These additional layers include the prevention and detection of unauthorized entry, presence, and movement of individuals and ground vehicles into, and within, the secured and Airport Operations Areas (AOA) 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 secured area. Examples of the security measures that may be employed at direct access points and airport perimeters include: Vehicle inspections, explosives trace detection of individuals and property, enhanced screening, accessible property searches, and identification/media verifications, as well as behavior detection.

BEHAVIOR DETECTION PILOT PROGRAM AT BOS

TSA has long recognized the value of a layered, threat-based approach to transportation security and the need to focus more of our resources on people we know less about who potentially pose a threat to aviation security.

As part of its on-going commitment to implement risk-based security measures, TSA is conducting a pilot program at BOS designed to assess the expanded use of behavior detection in the airport screening process. Extensive research indicates behavior analysis and interviewing are effective methods for detecting hostile intent and potential high-risk individuals. TSA's own behavior detection program, the Screening of Passengers by Observation Techniques (SPOT) program—whose indicators have been scientifically validated through research conducted by the DHS Science and Technology Directorate—revealed that behavior detection was effective for identifying persons attempting to defeat the screening process. BOS was the first airport in the country to implement the agency's SPOT program, which is now employed at more than 160 airports Nation-wide.

As part of the pilot, TSA is utilizing specially trained and certified Behavior Detection Officers (BDOs) who are focusing on increased passenger interactions and behavior analysis in conjunction with boarding pass and identification review at the entrance to the checkpoint. The advanced training the officers receive includes both classroom and on-the-job training designed to enhance their communication skills to engage in conversations with passengers to determine whether they pose a threat to transportation security. Although the vast majority of passengers will experience a casual greeting conversation with the BDO as they begin the security checkpoint screening process, a small number of passengers may be selected for an extended, but still limited, conversation and possibly for additional screening.

The goal of this pilot is to understand how behavior detection can be used to improve both the effectiveness of transportation security and the passenger experience. TSA will evaluate how this pilot program impacts security, screening operations and passenger throughput, among other things, and these results will help determine how the agency proceeds with the program.

COLLABORATION: AN ESSENTIAL COMPONENT OF SECURITY AT BOS

Collaboration is an essential component of transportation security. Since its creation, TSA has engaged Massport, the Massachusetts State Police, and the airline carriers in a cooperative and complementary effort to enhance security throughout Logan Airport, best exemplified by the daily morning security briefing. At this meeting, we discuss incidents of the previous day, new security measures, and plans for the coming days and weeks. It is an opportunity for everyone to share their views and concerns to reach a common understanding of roles and responsibilities.

Some of the tangible results arising from the cooperative atmosphere include:

- Massport and the State Police partnership with TSA assets to develop and execute "plays" that deploy varying security measures on a random basis throughout the terminals and the secure areas of the airport;

- In the event of an incident, TSA, Massport, State Police, and the affected carriers convene an immediate conference call to determine the facts, assess the risk, and jointly decide on a course of action to resolve the matter with as little disruption as possible to the continued operation of the airport;
- TSA and Massport have worked together to improve Closed Circuit Television (CCTV) coverage of the airport's critical areas, providing TSA officials with real-time access to all of the camera views from within TSA offices; and
- Cooperation extends across the Federal level as well, as illustrated by the creation of the Nation's first airport-based counterterrorism office. DHS components, including TSA, U.S. Customs and Border Protection (CBP), and U.S. Immigration and Customs Enforcement (ICE) will work at the FBI's newly-opened Joint Terrorism Task Force (JTTF) office at Logan Airport to improve communications on security-related tasks.

PERIMETER SECURITY: A SHARED RESPONSIBILITY

As required by statute, TSA prescribes procedures for screening individuals, and inspecting goods, property, vehicles, and other equipment before entry into the secured area of an airport. These security access regulations, directives, and procedures safeguard against unauthorized persons having access to aircraft, thereby reducing opportunities for criminal violence, sabotage, or other destructive acts. These safeguards help to ensure the safety and integrity of individuals involved in the aviation domain, including aircraft service providers and workers involved in catering and passenger amenities on-board aircraft. Similarly, TSA requires security access programs for vendors with direct access to airfields and aircraft. Ultimately, the airport authority is responsible for abiding by the perimeter security regulations set by TSA and must establish procedures for its personnel and resources, which may include law enforcement personnel, to ensure compliance with the regulatory requirements.

TRANSPORTATION SECURITY INSPECTORS MONITOR COMPLIANCE

TSA conducts on-going and comprehensive airport inspections to enhance security and mitigate risk associated with perimeter integrity, including Joint Vulnerability Assessments, conducted with the Federal Bureau of Investigations (FBI), regulatory Special Emphasis Inspections (SEIs) that focus on specific aspects of operations, and the testing of access control processes at airports. Based upon the results of these inspections and assessments, TSA develops mitigation strategies that enhance an airport's security posture and determines if any changes are required. TSA collaborates with airport operators to identify effective practices across the industry regarding access control and perimeter security.

To counter the potential risks to perimeter security, TSA deploys Transportation Security Inspectors (TSIs) to help 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 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. TSIs can recommend that civil penalties be assessed by TSA when repeated or egregious instances of noncompliance with regulations and security procedures are discovered.

Earlier this year, TSA's Office of Security Operations—Compliance Programs initiated a Special Emphasis Assessment (SEA) and an SEI of all Category X and Category I through IV airports, evaluating perimeter security, including fencing, non-fenced man-made barriers, natural barriers, CCTV, electronic intrusion and motion detection devices, and other barriers. Assessments are complete for all Category X and I airports and the remaining airport assessments are expected to be completed later this month.

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. We want to thank the subcommittee for the opportunity to discuss this important issue with you today and we are happy to answer any questions you may have.

Mr. MCCAUL. Thank you, Mr. McLaughlin.

The Chairman now recognizes Admiral Naccara for his testimony.

STATEMENT OF ADMIRAL GEORGE NACCARA (RET.), FEDERAL SECURITY DIRECTOR, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Admiral NACCARA. Good morning, Chairman McCaul and Ranking Member Keating. As my colleague, Chris McLaughlin, stated, I will now discuss TSA initiatives that are specific to security operations at Boston Logan Airport.

TSA has long recognized the value of a layered threat-based approach to transportation security and the need to focus more of our resources on people we know less about who may pose a threat to aviation security. As part of its on-going commitment to implement risk-based security measures, TSA is conducting a Proof of Concept here in Boston to assess the value of expanding behavior detection in the airport screening process. Extensive research indicates this process is effective for detecting hostile intent and potential high-risk individuals.

TSA's Behavior Detection Program, as you mentioned earlier, sir, the Screening of Passengers by Observation Technique, also known as SPOT, reveal that behavior detection was effective for helping identify persons attempting to defeat the screening process. Logan Airport was the first airport in the country to implement the agency's SPOT program, which is now employed at over 160 airports Nation-wide.

As part of this Proof of Concept, TSA is using specially trained and certified Behavior Detection Officers, called BDOs, who are focusing their efforts on passenger interactions and behavior analysis. This is also being done in conjunction with boarding pass and identification review at the entrance through the checkpoints. The advanced training the officers receive includes both classroom and on-the-job training, and they are designed to enhance their communication skills to engage in conversations with passengers to determine whether they may pose a threat to transportation security. Although the vast majority of passengers will experience a casual conversation with our BDOs, a small number of passengers may be selected for an extended but still limited conversation and some possibly for additional screening.

The goal of this Proof of Concept is to understand how behavior detection can be used to improve the effectiveness and efficiency of transportation security and also the passenger experience. We will evaluate how this Proof of Concept impacts security screening operations and passenger throughput, among other things, and these results will help us determine how the agency proceeds with the program.

Now, I would like to describe how we are cooperating with our other essential partners at the local level to closely coordinate our security efforts. As you mentioned before, collaboration is essential to strengthening transportation security. Since its creation, TSA has engaged MassPort, the State police, and the airline carriers here to enhance security throughout Logan Airport, best exemplified by our daily morning briefing.

As an explanation, at this briefing, we discuss incidents of the previous day, new security measures, as well as longer-term plans for the coming days and weeks. It is an opportunity for everyone in the security environment to share their views and concerns and to reach a common understanding of our roles and responsibilities in respect to security.

Many positive tangible results arose from this cooperative atmosphere, including a partnership with MassPort, the State police, and TSA to develop and execute plays that deploy varying security measures on a random basis throughout the terminals and secure areas of the airport allowing us to address vulnerabilities heretofore unaddressed.

In the case of a security incident, TSA, MassPort, State police and the affected carriers immediately convene a conference call to determine the facts, to assess the risks and to collaboratively decide on a course of action to resolve the matter with as little disruption to traffic as possible. TSA and MassPort have also worked together to improve the closed circuit TV coverage of the airport's critical areas, providing TSA officials and airport officials with real-time access to all available cameras in the airport.

This cooperation also extends across the Federal level as illustrated by the creation of the Nation's first airport-based counterterrorism office, as you've mentioned before. In that office, several DHS components, including TSA, the Customs and Border Protection, Immigration and Customs Enforcement, will all work with FBI's newly-opened Joint Terrorism Task Force office at Logan Airport. We will certainly improve communications, and this will also enhance intelligence sharing.

Thank you for your time, and I look forward to answering any questions that you may have, sir.

Mr. MCCAUL. Thank you, Admiral.

The Chairman now recognizes Mr. Freni for his testimony.

STATEMENT OF EDWARD C. FRENI, DIRECTOR OF AVIATION, MASSACHUSETTS PORT AUTHORITY

Mr. FRENI. Chairman McCaul, Ranking Member Keating, welcome to Boston Logan International Airport. I want to thank you for giving us the opportunity to describe some of the measures that we've taken at Logan Airport to emerge from the tragedy of 9/11 into an airport recognized by both the Federal Government and our peers in the airport industry as a National leader in aviation security.

For the record, my name is Edward C. Freni, and I'm Director of Aviation for the Massachusetts Port Authority which owns and operates Logan Airport as well as Worcester Regional Airport and Hanscom Field in Bedford.

Last Sunday, America marked the 10th anniversary of the worst terrorist attack on this country in our history. More than 3,000 of our fellow Americans, as well as many citizens from other nations, were brutally killed in New York City, Washington, DC, and in a remote field in rural Pennsylvania. One hundred and forty seven of those fatalities were from Logan Airport, as two flights departing Boston for Los Angeles on the morning of September 11, 2001, American Airlines Flight 11 and United Airlines Flight 175, were

commandeered by terrorists and used to attack New York's World Trade Center towers. Logan is a place where the scars left by the 9/11 attacks "still run deep," as security expert Stephen Flynn said, accurately, as I can attest.

September 11 had a profound impact on MassPort. Since that fateful day, MassPort has implemented an aggressive program of smart and focused security initiatives to strengthen defenses against potential threats. In the days and months following the attacks of 9/11, MassPort has worked tirelessly to implement strategies, policies, and programs suggested by security experts in the industry. MassPort continues to explore new technologies and ideas in order to maintain our status as a security innovator.

Logan responded to that challenge and is now recognized as a National leader in aviation security. Logan is frequently chosen by the TSA and the Department of Homeland Security to pilot new techniques and technologies before they're installed and implemented Nation-wide. Behavioral pattern recognition surveillance techniques were pioneered by our State police here at Logan. The TSA took note of this new technique, which is an adopted version of methods used by the Israelis to spot terrorists using information derived from observed behavior rather than racial or ethnic categories and transformed it into a National program that TSA calls SPOT.

Today, the TSA is again recognizing Logan's appreciation of this behavior approach by using us as their initial test site for risk-based screening using specially trained behavior assessors who ask passengers a short list of questions to help them determine if passengers might be pursuing a hostile agenda.

Logan was the first airport in the country to meet the 2002 Congressional mandate for 100 percent baggage screening when we completed on time an automated in-line system of screening all checked baggage. MassPort is also a leader in evaluating new transportation security technologies on its own. To help weigh the effectiveness of new technologies, MassPort's Office of Corporate Security created the Transportation Security Center of Excellence that invites inventors, vendors of emerging technologies to test their products at MassPort's airport and Seaport facilities.

Logan also tries to make security everyone's business, from the CEO to the front-line ticket agents and baggage handlers. We've even badged and deputized the clammers who fish in the mudflats off Logan's runway ends, recruiting them to be an additional set of eyes and ears, reporting suspicious activity out there in our vulnerable airport perimeter.

But the most significant improvement we've made toward keeping our airports and the flying public safer and more secure is the communication, coordination, and close working partnerships that now exist between agencies who have met every day since 9/11 to review the latest information and intelligence together and to plan an appropriate response for that day. MassPort's daily 8:30 morning security meeting bringing together all agencies with security responsibilities is well-known throughout the industry.

For the sake of simplicity, Logan Airport's response after 9/11 can be grouped under three broad categories. First were steps to physically harden Logan Airport and our other airport and seaport

facilities against the possibility of their being a target of direct terrorist attack such as a suicide bombing. Under this category, I must include the consolidation of 11 points of access to Logan airfield pre-9/11 into just 2 heavily fortified, military-style security gates post-9/11 capable of withstanding an attempted breach from even a heavy vehicle.

Second are the technological innovations we've made to the airport's security. Here I would like to include our baggage screening system, the biometric controlled access systems and surveillance cameras that we've installed, as well as the technologies we field-tested in real-time real-life settings including those screening technologies we pilot-tested for the TSA.

Third are the steps we've taken to marshal and better organize the human assets that protect this airport. That includes everything from the Massachusetts State Troopers from Troop F who patrol Logan's terminals to the Sky Caps who work the terminal curbsides. There is an old saying that goes, "You can't manage what you can't measure."

Also unique to Logan is the development and use of over 200 line items of security metrics that help MassPort manage its multi-million dollar security program. Our metrics enable us to achieve a high level of visibility on the performance of all our security program components and track their performance over time by comparing performance year over year. This has lead to many improvements such as the camera surveillance program current metric that no camera is out of service more than 24 hours on average.

Hardening Potential Targets: Let me begin with some of the steps we took physically to harden Logan Airport as a future terrorist attack. I've already mentioned the restricted access to the Logan airfield that now exists with a single heavily fortified gate at both the northern and southern ends of the airfield.

In addition, Logan erected pillars, concrete barriers in front of every terminal to prevent a terrorist from driving a bomb into the airport. We also replaced its 8-foot-high chain-link fence around the perimeter to a 10-foot-high concrete wall.

After 9/11, MassPort's security organization was thoroughly reviewed and analysis was completed of all of the procedures currently in place along with the placement and security of all fences, doors, windows, gates, underground utility tunnels, air intakes, and hundreds of smaller details bearing on the security of those critical assets.

While Logan's Nationally-recognized bag screening system garnered most of the attention and accolades, there were other equally important initiatives undertaken to improve the overall security of MassPort's facilities. Shatter-proof laminate was installed in every airport terminal window to reduce injuries from flying glass should an explosion occur. Hundreds of bomb-resistant trash receptacles were installed in all of our terminals and our parking garages. Barriers were erected to prevent vehicles from approaching sensitive buildings. Idling limos and taxis were relocated so that they could be screened away from the terminal areas before proceeding to pick up our passengers.

Tow trucks were deployed in forward positions alerting motorists that unattended or illegally parked vehicles at terminal curbsides

would be removed. This was especially true when the security threat level went up triggering MassPort's zero tolerance policy that compels the immediate impoundment of improperly parked vehicles anywhere on our property. A vehicle inspection system was instituted to reopen parking lots near terminals that were closed by order of the FAA after the terrorist attacks.

Authorized by a special act of the Massachusetts State Legislature, a 500-foot security zone was established around Logan's waterside perimeter. The perimeter is marked off with buoys and enforced by stepped-up patrols, which also gave MassPort an opportunity to strengthen our relationship with the U.S. Coast Guard, our local harbormasters, and the City of Boston's maritime security efforts. Random roadblocks were conducted by State police troops at the entrance points of our airport.

Technological Innovations: Logan Airport is also in the forefront of technological innovations used to improve security. Logan was the only Cat X airport to complete the project of December 31, 2002, Federal deadline, 4 years later remained among the few large airports to have achieved a fully in-line explosive detection system. This was among the achievements that helped Logan earn Air Safety Week Airport Security Report's Exceptional Performance of Airport Security in 2004.

Workers travelled to Logan from more than 40 States after 9/11 often sleeping in trailers they hauled themselves to install nearly 3 miles of bag belts, powered by more than 300 motors, construct 85,000 square feet of new bag rooms, renovate 55,000 square feet of existing bag rooms and construct eight new power substations.

Logan is also making the needed structural changes. We have also installed about 200 security cameras throughout every airport concourse and airfield access points that can be monitored simultaneously at one central security office. A high-resolution surveillance camera currently being tested in Terminal A can record activity in an area the size of a stadium all the way to a Coke spilled on the floor.

Along the airport perimeter, we have an extensive defense in depth which combines camera surveillance technology with police and fireboat patrols, police, fire, and operations vehicle patrols, and special fencing. We're also pursuing an automated intrusion detection system for this area. In 2007, we installed new access control systems to ensure that only authorized personnel are able to enter our secure areas.

Our Human Assets: Technology is an important tool, but more important are the people who use it. While new technologies and capital construction projects grab the headlines, good security starts with people, communication, and organization. Logan believes that security is everyone's business, from the MassPort's CEO to the hundreds of vendors who work in the terminals.

Through our Logan Watch Program, the airport instills a culture of security awareness among Logan's front-line staff, the eyes and ears of this airport who deal face-to-face with Logan's customers every day, by giving them counterterrorism training to help them spot and report activity that may be out of the ordinary or suspicious.

A list of employees to help guard against threats is important. But equally important is to ensure that prospective employees are not threats to themselves. This is why we instituted an intensive system of background checks and badging for everyone that works in this airport, whether in a secure area or the public space.

But perhaps the most important improvement made since September 11 has been the improved communication and cooperation that now exists among State, local, and Federal agencies that have responsibilities to keep Logan safe and secure.

Admiral Naccara, Major Concannon, and I were not merely picked at random to be on this panel. We are part of a much larger team which first met on the afternoon of September 11 and has continued to meet and is meeting every single morning since then at 8:30 to assess current security information and threat intelligence. Seven days a week, Logan's security team assembles, MassPort Operations security teams, MassPort Fire Rescue and the Massachusetts State Police, the FAA, the TSA, the FBI, the Federal Air Marshals Service, the U.S. Customs and Border Protection, the airlines, our major tenants, and construction contractors are among those who attend this meeting.

At the meeting, we review the events of the past 24 hours, set the priorities and actions for the coming day. This is tremendously effective because all of the key decision-makers are present in one room at the same time every day. All agencies can now simultaneously review intelligence from the preceding 24 hours and adjust our priorities and response for the day ahead.

In conclusion: From the challenges of 9/11, Boston Logan International Airport has emerged as a Nationally-recognized leader in airport security. The airport's layered approach to security creates a gauntlet of information-sharing, interagency cooperation, cutting-edge technology and top-to-bottom human interaction that helps identify and thwart potential threats to the safety and security of Logan's workers and passengers, whether from terrorism or other sources.

Logan was the first major airport in the Nation to have 100 percent in-line checked baggage screening, a 10-foot-high perimeter concrete wall around its landside boundary, a behavioral detection program that has been implemented and replicated by the TSA Nation-wide, and 100 percent biometric access control to restricted areas of the airport. The list of Logan's new security initiatives over the last 10 years is long, yet however many initiatives MassPort may have launched over the past decade since 9/11, security involves much more than formulating countermeasures to identify threats and vulnerabilities.

At its core, good security is an extension of leadership. The commitment to use scarce resources to meet potential threats when other competing demands crowd for attention, the skill to educate the public about its responsibilities for improved security and the trade-offs it must make in lost time and convenience if the system is to work, the consistency to maintain organizational vigilance despite the inevitable and the almost endless lulls and false alarms, this requires strong, consistent leadership for a security system to work. These have been the hallmarks of MassPort's efforts as it has become a leader in transportation security.

Last Sunday the Nation paused to honor the memories of those lives that were tragically lost on September 11, 2001 and paid tribute to the courage and dedication to the duty of the heroes and first responders of that day, many of whom have lost their lives. Memorials now exist at Ground Zero in New York City, at the Pentagon in Washington, DC, and in a remote field in Shanksville, Pennsylvania, and here at Boston Logan International Airport where the attacks of 9/11 were both a National tragedy and a personal one for all of us.

Yet I believe that the most fitting memorial we could make to those who were lost that day is to continue doing everything humanly possible to ensure that the tragedy which took their lives never happens again. With this committee's help, I'm confident that we will.

Thank you.

[The statement of Mr. Freni follows:]

PREPARED STATEMENT OF EDWARD FRENI

SEPTEMBER 16, 2011

Chairman McCaul, Ranking Member Keating, and Members of the committee. Welcome to Boston Logan International Airport.

I want to thank you for giving us this opportunity to describe some of the measures we've undertaken at Logan Airport to emerge from the tragedy of 9/11 into an airport recognized by both the Federal Government and our peers in the airport industry as a National leader in aviation security.

For the record, my name is Edward C. Freni, Director of Aviation for the Massachusetts Port Authority which owns and operates Logan Airport as well as Worcester Regional Airport and L.G. Hanscom Field in Bedford.

Last Sunday, America marked the 10th anniversary of the worst terrorist attack on this country in our history. More than 3,000 of our fellow Americans, as well as many citizens from other nations, were brutally killed in New York City, Washington, DC and in a remote field in rural Pennsylvania.

One hundred forty seven of those fatalities were from Logan Airport as two flights departing Boston for Los Angeles on the morning of September 11, 2001—Americans Airlines Flight 11 and United Airlines Flight 175—were commandeered by terrorists and used to attack New York's World Trade Center towers.

Logan is a place where the scars left by the 9/11 attacks "still run deep," as the security expert Stephen Flynn said, accurately, as I can attest.

I was the senior aviation official in charge at Logan that morning as our airport director at the time, Tom Kinton, was in Canada along with many other airport directors from around the world attending the annual conference of Airports Council International. I had just gotten off the phone with Tom telling him the weather was beautiful and everything was going smoothly when we first learned a plane had hit the World Trade Center.

At first we thought it was just a single engine private plane whose pilot had either lost control or become disoriented and veered tragically off course. But then we learned it was a commercial jetliner, and also that it had originated from Logan Airport.

Then the second plane hit. In those first few hours after two flights from Logan Airport were hijacked, we couldn't be sure whether Logan itself might also be a target for attack.

The rest of that day, and those that followed, were a blur. Though we could not know the precise details at the time, all of us who were there that day at Logan Airport knew that from that moment on, our world would never be the same.

The tragic fact that Logan will forever be linked to 9/11 means there is a "never again sense of mission," as Flynn called it, among those of us at Massport and throughout the law enforcement community in Boston to raise the bar on the way we manage the risk of a possible future attack at Logan Airport.

September 11 had a profound impact on Massport. Since that fateful day, Massport has implemented an aggressive program of smart and focused security initiatives to strengthen defenses against potential threats.

In the days and months following the attacks of 9/11, Massport brought in National and international security experts, including a team from Israel, to work with the authority in developing a program second to none.

Since then, Massport has worked tirelessly to implement strategies, policies, and programs suggested by security experts in our industry. And Massport continues to explore new technologies and ideas in order to maintain our status as a security innovator.

Because of what happened at Logan that day, Massport has always felt a special obligation and urgency to be on the forefront of whatever new techniques or technologies are out there that promise to make aviation more secure.

We have been, because we knew that Logan Airport would always be in the National spotlight with a public anxious to believe in the air travel system again that would use Logan as a yardstick to measure how far we'd come to improve the security of that aviation system.

Logan responded to that challenge and is now recognized as a National leader in aviation security. Logan is frequently chosen by the TSA and the Department of Homeland Security to pilot new techniques and technologies before they are installed or implemented Nation-wide.

Behavior pattern recognition surveillance techniques were pioneered by our State Police here at Logan. The TSA took note of this new technique—which is an adopted version of methods used by the Israelis to spot terrorists using information derived from observed behavior rather than racial or ethnic categories—and transformed it into a National program the TSA calls "SPOT."

Today, the TSA is again recognizing Logan's appreciation of this behavior approach by using us as their initial test site for risk-based screening using specially-trained behavior assessors who ask passengers a short list of questions to help them determine if passengers might be pursuing a hostile agenda.

Logan was the first airport in the country to meet the 2002 Congressional mandate for 100% baggage screening when we completed on time an automated, in-line system for screening all checked baggage.

Massport is also a leader in evaluating new transportation security technologies on its own. To help weigh the effectiveness of new technologies, Massport's Office of Corporate Security created the Transportation Security Center of Excellence that invites inventors and vendors of emerging technologies to test their products at Massport's airport and seaport facilities.

Logan also tries to make security everyone's business, from the CEO to the front-line ticket agents and baggage handlers.

We've even badged and deputized the clammers who fish in the mudflats off Logan's runway ends, recruiting them to be an additional set of eyes and ears, reporting suspicious activity out there on that vulnerable airport perimeter.

But the most significant improvement we've made toward keeping our airports and the flying public safer and more secure is the communication, coordination, and close working partnerships that now exist between agencies who've met every day since 9/11 to review the latest information and intelligence together and to plan an appropriate response for that day.

Massport's daily 8:30 morning security meeting, bringing together all agencies with security responsibilities, is well-known throughout the industry.

For the sake of simplicity, Logan Airport's response after 9/11 can be grouped under three broad categories:

First, were steps to physically harden Logan Airport, and our other airport and seaport facilities, against the possibility of their being a target of a direct terrorist attack, such as a suicide bomber. Under this category I might include the consolidation of 11 points of access to the Logan airfield pre-9/11 into just two heavily fortified, military-style security gates post-9/11 capable of withstanding an attempted breech from even a heavy vehicle.

Second, are the technological innovations we've made to the airport's security. Here, I would include our baggage screening system, the biometric-controlled access systems and surveillance cameras we've installed, as well as the technologies we've field tested in real-time, real-life settings, including those screening technologies we've pilot-tested for the TSA.

Third are the steps we have taken to marshal and better organize the human assets that protect this airport, and that includes everything from the Massachusetts State Troopers from Troop F who patrol Logan's terminals to the Sky Caps who work the terminal curbs outside.

There is an old saying that goes: "You can't manage what you can't measure." Also unique to Logan is the development and use of over 200 line items of security metrics that help Massport manage its multi-million dollar security program.

Our metrics enable us to achieve a high level of visibility on the performance of all our security program components and track their performance over time by comparing performance year over year. This has led to many improvements, such as the camera surveillance programs current metric that no camera is out of service for more than 24 hours, on average.

HARDENING POTENTIAL TARGETS

Let me begin with some of the steps we took to physically harden Logan Airport against a future terrorist attack. A facility like Logan Airport designed for easy public access and serving as many as 28 million passengers a year—77,000 passengers a day—is often called a "soft target" because the open and publicly-accessible nature of its mission presents unique security challenges for those who operate and protect them.

I have already mentioned the restricted access to the Logan Airfield that now exists, with a single, heavily-fortified gate at both the northern and southern ends of the airfield.

In addition, Logan erected pillars and concrete barriers in front of every terminal to prevent a terrorist from driving a bomb into the airport. We also replaced its 8-foot-high chain link fence around the perimeter with a 10-foot-high concrete wall.

After 9/11 Massport's security organization was thoroughly reviewed. An analysis was completed of all the procedures currently in place, along with the placement and security of all fences, doors, windows, gates, underground utilities tunnels, air intakes, and the hundreds of smaller details bearing on the security of these critical assets.

Deterrence and prevention, of course, are always the primary objective. But prudence dictates that it is also necessary to adopt measures to decrease the deadly toll of a terrorist attack should one be attempted.

While Logan's Nationally-recognized bag screening system garnered most of the attention and accolades, there were other, equally important initiatives undertaken to improve the overall security of Massport's facilities:

- Shatter-proof laminate was installed to every airport terminal windows to reduce injuries from flying glass should an explosion occur.
- Hundreds of bomb-resistant trash receptacles were installed in all terminals and parking garages.
- Barriers were erected to prevent vehicles from approaching sensitive buildings.
- Idling limos and taxis were relocated so they could be screened away from terminals before proceeding to pick up passengers.
- Tow trucks were deployed in forward positions, alerting motorists that unattended or illegally parked vehicles at the terminal curbside would be removed. This was especially true when the security threat level went up, triggering Massport's zero tolerance policy that compels the immediate impoundment of improperly parked vehicles anywhere on the property.
- A vehicle inspection system was instituted to reopen parking lots near terminals that were closed by order of the FAA after the terrorist attacks—another security initiative that provides significant customer service benefits for Logan's passengers.
- Authorized by a special act of the Massachusetts State Legislature, a 500-foot security zone was established around Logan's waterside perimeter. The perimeter is marked off with buoys and enforced by stepped-up patrols, which also gave Massport an opportunity to strengthen our relationship with the U.S. Coast Guard, local harbormasters, and the City of Boston's maritime security efforts.
- Random road-blocks were conducted by State police troops at the entrance to our parking garages.

TECHNOLOGICAL INNOVATIONS

Logan Airport is also in the forefront of technological innovations used to improve security.

Compelling proof of this commitment is Logan's baggage screening system.

Logan was the only Category X airport to complete the project by the December 31, 2002 Federal deadline and 4 years later remained among the few large U.S. airports to have achieved a fully in-line Explosive Detection System.

That was among the achievements that helped Logan earn Air Safety Week Airport Security Report's "Exceptional Performance in Airport Security Award" in 2004.

Logan's bag screening system was a massive undertaking successfully completed by nearly 800 bricklayers, electricians, carpenters, ironworkers, HVAC workers, bag belt workers, and others—all of whom had to be monitored daily to ensure secu-

rity—and who worked around the clock to compress 2 or 3 years of construction work into less than 1.

Workers traveled to Logan from more than 40 States after 9/11, often sleeping in trailers they hauled themselves, to install nearly 3 miles of bag belts powered by more than 300 motors, construct 85,000 square feet of new bag rooms, renovate 55,000 square feet of existing bag rooms, and construct eight new power substations.

Logan's was the first bag screening system given the go-ahead to begin construction on the Federally-mandated system by the new TSA, and Massport's Board committed nearly $150 million to expedite construction before the reimbursement formula that eventually repaid those funds was even in place.

At the same time the bag screening project was moving forward, Massport was designing and constructing modern security checkpoints for the TSA's passenger screening.

The system incorporated updated equipment, better layout for increased flow, and the development of exit lane security doors and video monitoring to prevent the need to empty a terminal or concourse should there be concern about a possible security breach. Since then Logan has made significant investments to improve efficiency by retrofitting our terminals to consolidate checkpoints in both Terminal B and Terminal C.

These are just a few examples where Logan is improving security with technology. Logan is also making needed structural changes.

We have also installed about 200 security cameras throughout every airport concourse and airfield access points that can be monitored simultaneously from a central security office. A high-resolution surveillance camera currently being tested in Terminal A can record activity in an area the size of a stadium, all the way down to a Coke spilled on the floor.

Along the airport perimeter we have an extensive defense in depth which combines camera surveillance technology with police and fire boat patrols; police, fire, and operations vehicle patrols, and special fencing. We are also pursuing automated intrusion detection for this area.

In 2007, we installed a new Access Control System to ensure that only authorized personnel are able to enter secure areas.

Logan also tries to be on the cutting edge of the development of new techniques and technologies to make our Nation more secure than it has ever been before. We have become a laboratory for the field testing of promising new security innovations. To separate what works from what's a waste of time Massport has assembled a special Security Advisory Committee.

This group of experienced professionals, with contacts in New England's academic and business communities, works with our Director of Corporate Security to evaluate new security technologies and how they might be used.

The council helps us to quickly decide which ideas are worth pursuing as we continue to launch pilot projects that push the envelope on ways to improve security—without sacrificing operational effectiveness.

These tests, for example, proved the value of handheld wireless computers that were issued to our State Police, allowing troopers on foot patrol to conduct criminal history and license plate checks via a secure wireless network.

HUMAN ASSETS

Technology is an important tool. But more important are the people who use it. While new technologies and capital construction projects grab the headlines, good security starts with people, communication, and organization.

Logan believes that security is everyone's business, from Massport's CEO to the hundreds of vendors who work in the terminals. To remind everyone of this fact and to keep workers vigilant and on their toes, Logan has instituted a public recognition program called "SAFE"—Security Awareness is for Everyone—to single out those workers who do their part to protect this airport.

Through our "Logan Watch" program the airport instills a culture of security awareness among Logan's front-line staff—the eyes and ears of this airport who deal face-to-face with Logan's customers every day—by giving them counter-terrorism training to help them spot and report activity that may be out-of-the-ordinary or suspicious.

To help employees do that more effectively, while also providing customer service benefits, Massport established an "English for Speakers of Other Languages" program at Logan Airport that has been in effect for the past 2 years. This joint effort of Massport, UGL Unicco, and SEIU Local 615 provides 32 weeks of intensive English instruction for airport workers whose primary language is not English.

With the emphasis Logan Airport places on front-line airport employees to provide clear and accurate information to law enforcement officials about potential threats to airport security and public safety, Massport knew it was important to improve the English proficiency skills of everyone who works at this airport.

While improving airport security may have been the primary impetus for a program that gives all airport workers the confidence to communicate effectively with the public, providing language skills also improves customer service for our passengers and opens new career doors for our workers.

Enlisting employees to help guard against threats is important. But equally important is to ensure that prospective employees are not threats themselves. This is why we have instituted an intensive system of background checks and badging for everyone who works at this airport, whether in secure areas or public spaces.

A program was implemented to check the fingerprints and criminal history records of all airport employees, contractors, and construction workers. These innovations don't stop at Logan Airport as Hanscom Field in Bedford became the first airport of its size to have a security badge program using FBI fingerprint background checks to better identify people who have access to the airfield.

These were just some of the measures Logan adopted after turning to Nationally and internationally respected experts on counter-terrorism in order to better understand and prepare for the new world we woke up to on the morning of September 11, 2001.

Airports in America have a lot to learn from the experience of airports in those parts of the world that have had to deal with the threat of terrorism much longer than we have. So immediately after 9/11 Logan hired the former head of security for Israel's El Al Airlines and Ben Gurion Airport, Rafi Ron, whose experience as a security specialist in one of the world's most dangerous regions was invaluable to Logan in preparing to counteract today's the new threats.

By bringing Rafi Ron to Logan Airport we have been able to learn about the strict security that is standard operating procedure in Europe and Israel, while learning how these security measures can be adopted and incorporated into the operations of large, complex American airports like Logan with their unique demands and constraints.

But perhaps the most important improvement made since September 11 has been the improved communication, cooperation, and cooperation that now exists among State, local, and Federal agencies that have responsibilities for keeping Logan safe and secure.

Admiral Naccara, Major Concannon, and I were not merely picked at random to be on this panel. We are part of a much larger working team which first met on the afternoon of September 11 and has continued meeting every morning since then at 8:30 to assess current security information and threat intelligence.

Seven days a week, Logan's security team assembles: Massport operations and security teams, Massport Fire Rescue, the Massachusetts State Police, the FAA, the TSA, the FBI, the Federal Air Marshal Service, U.S. Customs and Border Protection, the airlines, our major tenants and construction contractors, among others.

At the meeting we review the events of the past 24 hours and set the priorities and actions for the coming day. This is tremendously effective because all the key decision makers are present in one room, at the same time, every day. All agencies can now simultaneously review intelligence from the preceding 24 hours and adjust our priorities and response for the day ahead.

Another example of the close inter-agency cooperation you find at Logan Airport is the Joint Terrorism Task Force composed of Federal, State, and local law enforcement and security professionals.

In another security first, Massport and the FBI announced just last month the opening of a Joint Terrorism Task Force headquarters here at Logan International Airport—the first ever, airport-based FBI-Joint Terrorism Task Force Unit in the country.

Thanks to the new headquarters of the joint terrorism task force here at Logan, these agencies will be able to remain in constant physical contact even after the 8:30 morning meeting breaks up—further contributing to the teamwork that exists.

The offices, located on-site at Logan, were formally opened in July by FBI Director Robert S. Mueller III. The facility is a tangible example of the collaborative approach to security at this airport.

The agencies with a daily presence at the facility are the FBI, TSA, Federal Air Marshall Service, U.S. Department of State Diplomatic Security Service, U.S. Customs and Border Protection, Massachusetts State Police, Boston Police Department, Homeland Security Investigations, and Massport.

The opening of the JTTF Annex has greatly enhanced the task force's ability to share vital information and dramatically strengthen investigative support in a timely manner with those that may be affected by criminal acts.

CONCLUSION

From the challenges of 9/11 Boston Logan International Airport has emerged as a Nationally-recognized leader in airport security. The airport's layered approach to security creates a gauntlet of information-sharing, inter-agency cooperation, cutting-edge technology and top-to-bottom human interaction that helps identify and thwart potential threats to the safety and security of Logan's workers and passengers, whether from terrorism or other sources.

Logan was the first major airport in the Nation to have 100% in-line checked baggage screening, a 10-foot-high perimeter concrete wall around its landside boundary, a behavior detection program that has been replicated by the TSA Nation-wide, and 100% biometric access control to restricted areas of the airport.

The list of Logan's new security initiatives over the past 10 years is long. Yet, however many initiatives Massport may have launched over the past decade since 9/11, security involves much more than formulating countermeasures to identified threats and vulnerabilities.

At its core, good security is an extension of leadership. The commitment to use scarce resources to meet potential threats when other competing demands crowd for attention; the skill to educate the public about its responsibilities for improved security and the tradeoffs it must make in lost time and convenience if the system is to work; the constancy to maintain organizational vigilance despite the inevitable, and almost endless, lulls and false alarms—this requires strong, consistent leadership for a security system to work. These have been the hallmarks of Massport's efforts as it has become a leader in transportation security.

Last Sunday the Nation paused to honor the memories of those whose lives were tragically lost on September 11, 2001 and pay tribute to the courage and dedication to duty of the heroes and first responders of that day, many of whom also lost their lives.

Memorials now exist at Ground Zero in New York City, at the Pentagon in Washington, DC, in a remote field in Shanksville, Pennsylvania and here at Boston Logan International Airport, where the attacks of 9/11 were both a National tragedy and a personal one as well.

Yet I believe that the most fitting memorial we could make to those who were lost that day is to continue doing everything humanly possible to ensure that the tragedy which took their lives never happens again. With this committee's help, I am confident we will.

Thank you.

Mr. MCCAUL. Thank you, Mr. Freni. Let me just personally thank you for your service and the Massachusetts Port Authority for its service. I know you were here that fateful day. I can't imagine what was going through your mind, at that time. But you've been a real leader for the Nation, in terms of airport security, and you've really done a great job making this airport safer. So thank you so much.

Mr. FRENI. Thank you, Mr. Chairman.

Mr. MCCAUL. Next the Chairman now recognizes Major Concannon.

STATEMENT OF MICHAEL P. CONCANNON, MAJOR, STATE POLICE TROOP F, BOSTON LOGAN INTERNATIONAL AIRPORT

Mr. CONCANNON. Good morning, Chairman McCaul and Ranking Member Keating. It's my honor and pleasure to speak with this committee regarding the topic of assessing airport security and preventing a future terrorist attack. Thank you for this opportunity.

For the record, my name is Major Michael D. Concannon. I'm the Commanding Officer of Troop F of the Massachusetts State Police, charged with providing law enforcement and security services here

at Boston Logan International Airport as well as at other MassPort properties.

I'd first like to acknowledge the tremendous and professional working relationships that exists among the numerous entities that make up the security team at Logan Airport. It is my sincere belief that it is because of these incredibly strong partnerships that Logan Airport has been able to get it right when it comes to securing the large Category X international airport in the post-9/11 era.

Those of us who work hard each day to protect the people and infrastructure at Logan understand that nothing less than a true team effort will work. Clearly, there is a sensitivity at Logan Airport due to the history here that drives this high level of commitment. The exceptional professional and personal relationships that have been forged through the years here at Boston have laid the foundation for any number of historic and groundbreaking security enhancements.

Among these achievements are an historic playbook collaborative effort, an effective and coordinated State police and TSA canine effort, a comprehensive advanced imaging testing resolution protocol, an effective and efficient coordinated effort to maximize the resources of the TSA's bomb appraisal officers, as well as our own bomb squad, a practical and legally sound checkpoint response protocol, a unified breached resolution protocol, an on-airport robust ICE/DEA task force, and a recently established first in the Nation on-airport FBI Joint Terrorism Task Force Annex. These are just some of the advancements that we've been able to implement here at Logan Airport in recent years, and they are an example of, as well as, the fruits of the solid partnerships in place here at Logan.

We continue to cultivate a very positive culture within the Logan security team where all of the airport's stakeholders, each and every employee is expected to understand, appreciate, and perform a security rule. These efforts were recently recognized at the highest levels of the TSA when the newly-appointed administrator, Mr. John Pistole, on his very first airport visit upon being appointed came to Logan Airport. He commented that the security operation here was "one of the best, most secure" of all of the airports in the Nation. We strive each day to ensure that our efforts are worthy of such high praise.

In my role as Troop F Commander, I'm involved in all security matters that concern Logan Airport as well as other MassPort properties, and I work every single day with all of our partners, most notably, the TSA. In addition to being the Troop F Commander, I also serve as MassPort's Director of Aviation Security, and I'm afforded a seat at the table for all security-related discussions.

The specific assets that the Massachusetts State Police offer in protecting these properties are numerous. Troop F consists of several components, including uniform troopers who perform patrol duties, troopers in tactical units such as the bomb squad and canine units, as well as troopers in investigative units and support units. We also have an officer assigned full-time to the newly created JTTF Annex. Each officer views his or her role as a member of the larger airport community and has embraced the cooperative

and collaborative approach that is so vital in protecting the airport, its stakeholders, and the traveling public.

Troop F is different from other geographic troops that make up the Massachusetts State Police, most of which include among their duties patrols of long stretches of State highways. While Troop F does not have the traditional patrol function, we do have the unique responsibility for maintaining a layered security approach at Logan Airport including the waterside and landside perimeters, the terminal and curb area, both with the public side of the passenger terminals and the sterile side as well as the aircraft operating area, the ramp area. The focus at Troop F primarily here at Logan Airport is a blend of a proactive security strategy coupled with a strong customer service approach. Our goal is the professional delivery of the highest levels of police and security services to MassPort through a combination of vigilance and courtesy.

Not only is the specific mission of Troop F different than other State police troops, but the approach to fulfilling the mission is also different. Rather than a traditional response model whereby police officers respond to calls for service after the fact, the model at Troop F is a proactive one. Every officer here, regardless of unit assignment, has been trained in behavior pattern recognition and is expected to utilize these skills on a daily basis throughout the airport. Troopers are expected to be alert for anything or anybody who appears out the ordinary, whose behavior does not seem to fit in with normal actions and routines of travelers. When such behavior or action arises or raises questions, troopers engage that person in conversation to further assess the situation. This proactive preventative approach to security is certainly different than many of the assignments on the State police, and this mind-set is reiterated and reinforced repeatedly here at Troop F.

Boston Logan was the first airport in the Nation to deploy this BPR program which was modeled after the Israeli airport security program and has been adapted for U.S. airport environment by Mr. Rafi Ron, an international aviation security expert hired by MassPort immediately after 9/11. The BPR program contributes to the creation of an efficient multilayered security system for the airport. As has been mentioned, this concept was the forerunner of the SPOT EDO program that you've heard about.

It should be pointed out that, whenever a new security strategy is introduced, its vital to ensure that the Security team is on the same page. Beyond that, it's also critically important that the public supports the efforts as well.

The BPR program and its observation and conversation techniques have been well-received at Logan Airport and have been embraced by the entire security team. These techniques are welcome by Logan Airport passengers who are reassured by the proactive and professional approach designed to identify potential criminals or terrorists without inconveniencing the tens of thousands of passengers who use Logan Airport each day. Not only are the officers of Troop F trained to be on the lookout for items, persons, or behaviors of concern, they are also trained to receive any and all referrals by airport employees and members of the public of issues that concern them.

We coordinate our efforts closely with a variety of law enforcement and Homeland Security partners, including MassPort, the TSA, the Federal Air Marshals Service, Customs and Border Protection, the FBI, Immigrations and Customs Enforcement and the DEA, just to name a few. The officers assigned here in each of our security partners understand and accept that we are all part of a much larger layered security framework at the airport that includes not only law enforcement, public safety, and security personnel but also every single one of our 14,000 badged airport employees. The mind-set of every single person who works at the airport must be and is, "If you see something that concerns you, you should say something to the authorities," or in short, "See something, say something."

Further, it's often mentioned here that, if you work at Logan Airport and you can go a day without thinking of 9/11, you should not work at Logan Airport. This cannot be overstated. We rely heavily on the eyes and ears of the airport community, including the airline employees, the airport vendor employees, the ground transportation team and members of the traveling public to assist us in securing Logan Airport. We constantly remind each of these partners of the important role that they play, and we have programs in place to train these people, remind these people, and recognize these people for their contributions.

I'm confident in saying to this committee that the entire Boston Logan International Airport security team has worked very hard each day to accomplish these goals, and we have remained positive and flexible as we've had to adapt to evolving threats and challenging times. Further, we will continue to work hard and to be constantly mindful of the critical need for cooperation, communication, and collaboration. We have wrestled with many of the issues affecting airports across the country. But because of the constant effort to work together, to communicate openly, and to be mindful that we share a common goal, we have been able to work these issues to successful resolution.

The advice that we would offer to other airports is this: Communication serves to establish relationships. Relationships forge true partnerships. Strong partnerships ensure successful collaborative outcomes.

Again, I thank the Chairman and Ranking Member, Mr. Keating, and the committee for the opportunity to appear before you today and to share my thoughts. I look forward to any questions that you may have, thank you.

[The statement of Mr. Concannon follows:]

PREPARED STATEMENT OF MAJOR MICHAEL P. CONCANNON

SEPTEMBER 16, 2011

Good morning Chairman McCaul, Ranking Member Keating, and Members of the committee.

My name is Major Michael P. Concannon. I am the Commanding Officer of Troop F of the Massachusetts State Police; charged with providing law enforcement and security services here at Boston/Logan International Airport as well as at other Massachusetts Port Authority (Massport) properties.

It is my honor and pleasure to speak with this committee regarding the topic of assessing airport security and preventing a future terrorist attack. Thank you for this opportunity.

I would first like to acknowledge the tremendous professional working relationships that exist among the numerous entities that make up the "Security Team" at Logan Airport. It is my sincere belief that it is because of these incredibly strong partnerships that Logan Airport has been able to "get it right" when it comes to securing a large Category X international airport in this post-9/11 era.

Those of us who work hard each day to protect the people and the infrastructure at Logan understand that nothing less than a true team effort will work. Clearly, there is a sensitivity at Logan Airport, due to the history at our airport, that drives this high level of commitment.

The exceptional professional and personal relationships that have been forged through the years here at BOS have laid the foundation for any number of historic and ground-breaking security enhancements.

Among these achievements are: An historic Playbook collaborative effort, an effective and coordinated MSP and TSA K–9 effort, a comprehensive Advanced Imaging Testing (AIT) resolution protocol, an effective and efficient coordinated effort to maximize the resources of the TSA Bomb Appraisal Officers (BAO's), a practical and legally sound checkpoint response protocol, a unified breach resolution protocol, an on-airport robust ICE/DEA task force, and a recently established, first-in-the-Nation on-airport FBI Joint Terrorism Task Force Annex.

These are just some of the advancements that we have been able to implement here at Logan Airport in recent years and they are an example of (as well as the fruits of) the solid partnerships in place at Logan Airport.

We continue to cultivate a very positive culture within the Logan security team where all of the airport stakeholders, each and every employee, is expected to understand, appreciate, and perform a security role.

These efforts were recently recognized at the highest levels of the Transportation Security Administration (TSA) when the newly-appointed administrator, Mr. John Pistole, on his very first airport visit upon being appointed administrator, came to Logan Airport. He commented that the security operation here was "one of the best/most secure" of all the airports in the Nation. We strive to ensure that our efforts are worthy of such high praise.

In my role as Troop F Commander, I am involved in all security matters that concern Logan Airport, as well as all other Massport properties and I work every single day with all of our partners, most notably the TSA. In addition to being the Troop F Commander, I also serve as Massport's Director of Aviation Security and I am afforded a seat at the table for all security-related discussions.

The specific assets that the Massachusetts State Police offer in protecting these properties are numerous. Troop F consists of several components, including uniformed Troopers who perform patrol duties, Troopers in tactical units such as the bomb squad and K–9 unit, as well as Troopers in investigative units and support units. Each officer views his/her role as a member of the larger airport community and has embraced the cooperative and collaborative approach that is so vital to protecting the airport, its stakeholders, and the travelling public.

Troop F is different from other geographic Troops that make up the Massachusetts State Police, most of which include among their duties patrols of long stretches of State highways. While Troop F does not have the traditional "patrol" function, we do have the unique responsibility for maintaining a layered security approach at Logan Airport, including the waterside and landside perimeters, the terminal curb area, both the public side of the passenger terminals and the sterile side of the terminals (post screening), and on the ramp areas (the aircraft operating area—the AOA).

The focus at Troop F, primarily at Logan Airport, is a blend of a proactive security strategy coupled with a strong customer service approach. Our goal is the professional delivery of the highest levels of police/security services to Massport, through a combination of vigilance and courtesy.

Not only is the specific mission of Troop F different than the other State Police Troops, but the approach to fulfilling that mission is also different. Rather than the traditional "response" model, whereby police officers respond to calls for service (after the fact), the model at Troop F is "proactive".

Every officer at Troop F, regardless of unit assignment, has been trained in Behavior Pattern Recognition (BPR) and is expected to utilize these skills on a daily basis, throughout the airport.

Troopers are expected to be alert for anything or anybody who appears out of the ordinary, whose behavior does not seem to fit in with normal actions and routines of travelers. When a behavior or action raises questions, Troopers engage that person in conversation to further assess the situation. This proactive, preventative approach to security is certainly different than many of the assignments on the State Police and this mindset is reiterated and reinforced repeatedly.

Boston/Logan was the first airport in the Nation to deploy this program, which was modeled after the Israeli airport security program and has been adapted for a U.S. airport environment by Rafi Ron, an international aviation security expert hired by Massport immediately after 9/11. The behavior pattern recognition program contributes to the creation of an efficient, multi-layered security system for the airport.

Whenever a new security strategy is introduced, it is vital to ensure that the security team is on the same page. Beyond that, it is also critically important that the public supports the effort as well. The BPR program and its observation and conversation techniques have been well received at Logan Airport.

These techniques are welcomed by Logan Airport passengers who are reassured by the proactive and professional approach designed to identify potential criminals or terrorists without inconveniencing the tens of thousands of passengers who use Logan each day. They are viewed as a significant improvement over the random searches that were such a frustrating intrusion and inconvenience for the vast majority of passengers in the past. Not only are the officers of Troop F trained to be on the lookout for items, persons, and behaviors of concern, they are also trained to receive any and all referrals by airport employees and members of the public of issues that concern them. We coordinate our efforts closely with a variety of law enforcement and homeland security partners, including Massport, the Transportation Safety Administration (TSA), the Federal Air Marshals Service (FAMS), Customs and Border Protection (CBP), the Federal Bureau of Investigation (FBI), Immigration and Customs Enforcement (ICE), and the Drug Enforcement Administration (DEA) to name a few.

Troop F and the officers assigned here and each of our security partners understand and accept that we are all part of a much larger layered security framework at the airport that includes not only the law enforcement/public safety/security personnel, but every single one of our 14,000 Secure Identification Display Area (SIDA) badged airport employees. The mindset of every single person who works at the airport must be (and is) "If you see something that concerns you, you should say something to the authorities. Or, in short, "See Something, Say Something". Further, it is often mentioned that, "if you work at Logan Airport and you can go a day without thinking of 9/11, then you should not work at Logan Airport".

This cannot be overstated. We rely heavily on the eyes and ears of the airport community, including the airline employees, the airport vendor employees, the ground transportation team, and members of the travelling public to assist us in securing Logan Airport. We constantly remind each of these partners of the important role that they play and we have programs in place to train people, remind people, and to recognize people for their contributions.

I'm confident in saying to this committee that the entire Boston/Logan International Airport security team has worked very hard each day to accomplish these goals and we have remained positive and flexible as we've had to adapt to evolving threats and challenging times. Further, we will continue to work hard and to be constantly mindful of the critical need for cooperation, communication, and collaboration.

We have wrestled with many of the same issues affecting airports across the country, but because of the constant effort to work together, to communicate openly, and to be mindful that we share a common goal, we have been able to work these issues to successful resolution. The advice we would offer to other airports is this: Communication serves to establish relationships, relationships forge true partnerships, and strong partnerships ensure successful, collaborative outcomes.

Again, I thank the Chairman and the committee for the opportunity to appear before you today and to share my thoughts and I look forward to any questions that you may have.

Thank you.

Mr. MCCAUL. Thank you, Major, and I appreciate your testimony.

Now, you can't come to this airport without remembering what happened 10 years ago. You know, it was a bright, sunny day, a crisp day, not unlike today, that turned into one of the darkest chapters in American history. To sit here and to think not too far from where we sit, Mohamed Atta and his band of hijackers slipped through detection, slipped through our security and got onto those airplanes and proceeded to kill 3,000 people gives me a tremendous sense of sorrow but also of obligation to make this place more se-

cure. I will say, I think you all have done a fantastic job in that effort.

Since that day, we've become accustomed, as a people, to go through airports. We take our shoes off. We go through secondary screening. We go through pat-downs. It's just become a way of life.

As a Member of Congress—and I'm sure Mr. Keating as well—we often hear complaints about, you know, "Why are you taking the elderly woman aside and patting her down?" And "Why are you taking the child and patting them down?" "Why are you treating all Americans as an equal threat?"

Should we be more risk-based? Should we be looking more at the real threat rather than the grandmother? I think that's a common-sense approach, and I think that's an approach that this Behavior Detection Program, I think, seeks to do. Looking not at every individual as an equal threat, but let's look at the behavior of the individual. Is it suspicious? Let's analyze the behavior to spot those potential threats.

I've had numerous people say, "Why aren't we doing what they do in Israel? That works so well." I think that's what this program, as has been testified to, is really, it's part of that program. You all looked at what the Israelis have done, taken that and applied it here at Logan Airport. The first model, the first pilot program was done here. In my view, it's been successful, and now it's adopted in 160 airports across the country. It's resulted in 2,000 arrests in our airports. Again, I think it's just common sense.

So I just would like, I think it would be interesting to hear a little bit more about how this program works and how we can get beyond the day where the grandmother is patted down, the World War II Veteran is patted down, and the child is patted down.

Mr. Freni.

Mr. FRENI. As we stated, Mr. Chairman, shortly after 9/11, we had to strategize and make sure that we were doing the right things that made sense to make sure that this airport was secure.

Obviously, we thought that it was important that we take a look at the people that travel through the airport day-in and day-out. So we had engaged with Rafi Ron, as the Major mentioned in his remarks, to come in and show us the Israeli model. We thought that that fit appropriately. We decided, at that time, that we would train the entire Troop F in those techniques.

Along with that, we instituted a program called Logan Watch where the condensed version of that training is now introduced to all our employees that hold badges. They have to take that program before they are enabled to get a badge to work here at the airport. So they have the same knowledge that Mr. Ron had when he came to the State police group, so that they look to see if there is anything out of the ordinary on a daily basis. But we have drilled that into the fabric and imbedded it into the fabric of the way we do business here.

It's great to see that the TSA has now taken that program and instituted it with the size of the workforce that George Naccara has here. So that gives us a whole different group of people that are in the front lines that can look and pay attention to the behavior of those who come through our terminals and get on our airplanes.

So the SPOT Program is a derivative of what we did originally with Rafi Ron.

We welcome the opportunity to test the risk-based assessment that we have actually started and I'm sure George will talk about. But we are now exempting the young children under 12, so hopefully, your young son will be exempt from some of the scrutiny that some of the young children have had to go through, and it pains us to see that. Also, with the elderly group, we hope that it will branch out to that.

But the important thing is that we're watching and paying attention to the way people behave. We think that with the institution of the SPOT Program and other risk assessment programs that we're willing to test here any time at this airport is the best way to go.

Mr. MCCAUL. Well, thank you. You did mention my son. This was yesterday, I'm at Dulles Airport. He broke his finger playing football, so he had a metal splint, and of course went through the magnetometer and went through secondary screening, and he was tested for explosives. I don't know, I don't think my son is a threat to the National security of the United States. But in any event, it's good to hear that this airport is using that common-sense approach where you don't have to pat down 5-year-old kids.

I think that it will go a long way with the American people. They can accept having to go through a lot of this stuff. But when they see the grandmother or the child, I think they lose their patience with that. I think what you're doing will take this in the right direction.

You know, in oversight, we're often very critical. This is one of those days where I have to commend and applaud you for your efforts. Admiral, I want to applaud you for taking this, this model approach that the Israelis developed, and applying it throughout the Nation through the TSA.

Do you have any comments or would you like to explain how this works and what the training is?

Admiral NACCARA. Well, thank you, Mr. Chairman. I'll defer some of the explanation to my colleague, Chris McLaughlin, for the National approach to the risk-based security.

But as far as Logan Airport goes, what Mr. Freni explained was accurate. That was, we saw great value in what the State police were doing and what MassPort was doing here, and as an agency, we were leaning forward and looking for opportunities to improve security and perhaps to work away from complete reliance on technology and look into the human interaction and how that could enhance our processes.

Fortunately, we began with pilot programs here in 2005, expanded to other airports in the New England area. Then our headquarters understood and allowed us to begin a formal pilot program which has led to the Nation-wide SPOT Program that we have today with nearly 3,000 officers at around 160 airports.

Now, in the evolution of the human interaction and behavior detection, it's an exciting time. As you suggested, we are treating everyone the same, and that is not the most effective use of resources. So we need a method to assess the risk associated with

every passenger and then to manage that risk appropriately, and that's where we're headed.

Frankly, the Proof of Concept we have in place here is exciting and very well-embraced by MassPort and the State police and the carriers, which is critical to our success certainly, but even to the passengers. We've had this in place now for nearly 6 weeks. We've spoken to thousands, tens of thousands of passengers, and generally, the reaction has been extremely positive. The questions they're being asked are very similar to those which are asked of international passengers. Anyone who has traveled around the world has also been exposed to those types of questions. We're looking for the reactions, the behaviors, and we're also looking for inconsistencies in their story. That is refining our process so that we will treat people differently.

There are a number of elements to the overall program of risk-based security, and one of them addresses the issue of your child. Again, I'll allow Chris to talk about that. But that was a program that was piloted here and at five other airports around the country beginning about 6 weeks ago. There is some relaxation of the standards for children who appear to be 12 and under, and it's working very well.

Our goal, of course, is to minimize the pat-downs that are conducted on a child 12 and under. As you suggested, they are considered a much lower risk. We are adapting our systems. The World War II veterans you've suggested also, we've modified the processes for them as well. That's certainly deserved, and it's appropriate respect for them.

Mr. MCCAUL. That's right.

Admiral NACCARA. It's an exciting time for all of us, and you'll see many changes. They won't come too quickly, but on the other hand, the process has begun, and I'll defer to Chris on that.

Mr. MCCAUL. Let me just say that 10 years after the tragic events, this is certainly, in my judgment, a good news story.

Mr. McLaughlin, do you have any comments?

Mr. MCLAUGHLIN. Thank you, sir.

Coming up here from the District of Columbia, I mean, the first thing that I would like to do is truly recognize the local team here. They truly embody what we're looking for across the Nation in terms of a real partnership to securing our aviation process. So I'm honored to be here with them.

From literally his first day or first few days on the job, our administrator, John Pistole, has been talking actively about moving away from a one-size-fits-all security model to a risk-based approach. To that end, TSA has been working diligently on a number of different initiatives within the portfolio of risk-based security to try to do three things; improve security, do it more efficiently, and frankly, do it in a way that also improves the overall customer experience. We believe, truly, that we can accomplish those three things by taking a smart approach.

We learned from the support and the recommendations of the GAO with the variety of things that we roll out, we apply some of those pieces into the work we're doing, and we pilot them in places like Logan. At the end of the day, we are confident that things like the Assessor Proof of Concept, as we've shown recently with the pi-

lots with children under 12 and have now rolled out nationally, there are ways that we can look at an individual based on what we know about them in advance of their arrival to the airport, what we learn about them while they're at the airport, and then we can apply appropriate screening measures to them based on what we found out through that process.

So we agree wholeheartedly that there is a better, smarter, more effective, and more efficient way to doing this.

Mr. MCCAUL. Well, I look forward to getting updates on the successes. I know you've had 2,000 arrests. Fortunately, none of those were terrorist-related, although some involved, I think, counterfeit documents which could have been related to terrorism. But certainly, that's 2,000 criminals off the street.

So Major, as you had mentioned, I was a Federal prosecutor. I used to work with the JTTF, Joint Terrorism Task Force. It's a valuable model approach. You say that you are now very coordinated with their efforts here at the airport?

Mr. CONCANNON. Yes, we are, sir.

Mr. MCCAUL. Could you elaborate on that?

Mr. CONCANNON. Yes, Mr. Chairman.

We have a sergeant, one of our troopers, assigned full-time with the JTTF working closely with that team. The JTTF Annex here at the airport obviously has a close relationship with the Boston JTTF Annex downtown. They work closely on any issues that arise here at the airport. Our sergeant who is assigned there is able to bring back information to share with the troops. That can help with either an on-going investigation or certainly intelligence updates, things to be on the lookout for. We found it very productive. We think it's a great idea, and we'd like to see it expanded throughout the country.

Mr. MCCAUL. That's very good.

Mr. Lord, the 9/11 Commission's Tenth Anniversary Report Card had some criticism. We're still vulnerable to aviation security threats, in their opinion, and specifically talk about the need to improve screening at checkpoints using biometrics and standardized identification documents.

What are your thoughts on that?

Mr. LORD. Well, first of all, we've done a large body of work on, not only the screening process, but the technologies that's utilized to implement some of the processes. We found some problem areas in deploying effective technology, but also in using biometrics.

We did a very detailed assessment—it's not in the aviation sector, mind you, it's in the maritime—on the so-called TWIC biometric card. It's a Transportation Worker ID card. At one time, that was envisioned as the model. It was going to be rolled out across all modes of transportation. But they had some difficulties designing the card, implementing it, doing effective background checks. It proved to be a little more difficult than I think people originally envisioned.

Also, it's just being used a visual flash pass now. So we've had some covert investigators visit various ports, and they were able to obtain access to most of the facilities they entered. So our point was, well, until they're used with readers, it's really not going to be an effective deterrent. You need to, you know, make sure all in-

dustry stakeholders are on board before rolling out these types of programs.

Mr. MCCAUL. Go ahead.

Mr. LORD. Also, one additional point about the Israeli model. I probably get that question more than anything, regarding our work on behavior detection. I salute TSA's efforts to make the program more conversational. I think that has the potential to make it more effective.

But I think that it's important to also note that in Israel, they have a very small-scale size operation. So you have to be careful about inferring everything is readily transferrable to the U.S. model. Also in Israel, you can profile people, you know, on the basis of race, sex, and national origin. Obviously, that's a major difference between their system and our system which makes it, you know, less comparable.

Mr. MCCAUL. Of course, my opinion is the hijackers came from a certain part of the world, and our intelligence assets overseas are in those areas. I think that certainly, in my view, should be a factor.

But having said that, I do know that when I asked the Secretary why we're not using this approach, the Israeli approach, she said that it would take too long to process with, you know, millions of passengers. The good news, from what I understand through this program, it has not slowed down the process in any way, shape, or form.

Is that correct, Admiral?

Admiral NACCARA. Yes, sir.

As a matter of fact, we are testing various options. We call it a Proof of Concept. That allows us to explore different manipulations in this system. We're looking at the outcome, and one of those considerations in the outcome would be the through-put. So we've tried two different models, and in each case, we have seen virtually no difference in the overall screening process out in front. These are exciting times. We'll continue to test other models as well.

As Chris has pointed out, we have to be aware of different circumstances and different airports, certainly even in different checkpoints, and we have different levels of staffing. So those factors have to all be considered as we assess the data that comes in, and then we make some decisions as to where we go in the future. But this is very preliminary.

Mr. MCCAUL. I just want to follow up on the 9/11 Commission again, Mr. Lord.

When you say "readers," you're talking about, these are identification documents that can be falsified or used by another person to gain access to the airport, and you're talking about biometric?

Mr. LORD. Yes. These are biometric card readers.

Mr. MCCAUL. So it's the individual. You know that's the individual with the card.

Mr. LORD. Yes.

Everybody gets a card thing. Then to make it effective, you have to swipe the card to get access. In the TWIC program anyway, they've given everybody a card, but the readers aren't installed yet, so.

Mr. MCCAUL. Last question. I want to give my Ranking Member some time, and I appreciate your generosity.

I just want to end with a general question, and that is, you know, I was Chief of Counterterrorism at Justice for a while. I remember in 1993, Ramzi Yousef, World Trade Center bomber, escaped and went to Islamabad. I know the FBI agent who arrested him. When they knocked his door down, it was sort of eerie. He had baby dolls in his apartment, and they were stuffed with chemical explosives. His intention of the plot was to carry those baby dolls on multiple airlines and blow up simultaneously these airplanes. I know that his uncle, Khalid Sheikh Mohammed, had talked about flying airplanes into buildings in the mid-1990s.

The threat of chemical explosives is still an issue today. In fact, you know, just recently, the Christmas bomber, we know out of Yemen, the Clerk Yemen is still looking at ways to use chemical explosives on aviation to bring down airplanes. I think since that time, we've had another type of screening device.

So where are we with detecting chemical explosives, and what is the threat today from that, I guess, part of the question for the TSA?

Mr. MCLAUGHLIN. I'll take that question.

I have to confess that that's a bit beyond my scope of expertise in terms of the overall chemical threat in terms of the composition. What I will tell you is that threat does still exist, as you've pointed out, and really what you're talking about is the complexity of our issues.

So we're doing everything that we can to minimize intrusive techniques for the majority of customers, but we have to be cognizant of things like what you just described with baby dolls. So whether that's liquids, gels, or children's toys, we still have to make sure that every change that we make in a risk-based posture doesn't ignore the real threat that is very much there today. We're charged with defending against that.

Mr. MCCAUL. All right.

Mr. MCLAUGHLIN. So that the short answer is that we analyze each of our pieces as we roll in changes to our system to make sure that we're not missing something like a current and active threat.

Mr. MCCAUL. Thank you.

Admiral, do you have any comments on that?

Admiral NACCARA. We also have deployed certain pieces of technology at our checkpoints and in our baggage rooms to help us detect additional chemicals or explosives, what would be indicators of explosives. We're always improving that.

With each year, I think we've rolled out some new technologies that give us more capabilities. So as Chris suggests, it's a continuing process, and it's a challenge to keep up with the bad guys, frankly. But we have been attempting that. You'll see new pieces of equipment, periodically, at the checkpoint and in the baggage rooms.

Mr. MCCAUL. Thank you. I want to thank the Ranking Member for his patience. I hope I didn't ask every question that you were going to ask.

Mr. KEATING. No, thank you.

Mr. MCCAUL. With that, I recognize my good friend and colleague, Mr. Keating.

Mr. KEATING. Thank you, Mr. Chairman.

You know, Logan's perimeter security is unique, because there are so much water boundaries that are there, water-based boundaries. But there are airports in urban areas, airports in rural areas. So many airports have a different, you know, set of logistics attached to it.

One of the things cited in the 9/11 Commission report review touches on an area of concern that I have on—getting back to the Charlotte Douglas example with Delvonte Tisdale—you know, the issue they brought forward is the unity of command and who is in charge and making sure those lines are clear. The aviation director from Charlotte Douglas Airport where it was believed Mr. Tisdale breached perimeter security recently provided written testimony to Congress. He stated in that testimony, "When there is a threat on board an aircraft, the FBI responds and investigates. When a pilot makes an error on the aircraft, the FAA responds and investigates. And when there is an airplane crash, the NTSB responds and investigates."

If it's believed there is a security breach at a major U.S. airport, why shouldn't TSA respond and investigate first? Why, in that instance, was it first handed over to local police authorities to look at this? Shouldn't there be that same chain of command immediately where there is one Federal agency that just initiates and takes charge of that rather than turning to a local police authority?

Mr. MCLAUGHLIN. So I'll use Charlotte as the example, but I'll speak in more broad terms.

As I believe I stated earlier, TSA's role in airport security is to regulate a process. Each individual airport is required to write and operate in accordance with a local airport security program that TSA approves. The actual day-to-day oversight of the security operation in that airport does fall back to the airport authority.

What TSA does, and in this example, we use a finding from a breach such as happened in Charlotte. As an example, as a result of that, we conducted a National special emphasis inspection of all airports, from Cat X all of the way through Cat 4s. As I said, we'll be done with that analysis at the end of this fiscal year so that we can ensure that, once we've identified a problem, it doesn't happen again.

At the local level, we conduct annual and comprehensive inspections of the airports to ensure that they're in compliance with their plan. As we stated, we do perform joint vulnerability assessments at the required 34 airports a year, plus an additional between 10 and 15, depending on our resources. While that doesn't cover every airport, it certainly covers more than 75 percent of the traveling public that originate from those largest airports.

Mr. KEATING. I just think that, you know, there has been two repeated—well, there has been repeated breaches since then at that same airport and perimeter security.

Someone was breaching security stealing, from my understanding, diesel fuel out of the place, and that was happening, and someone else just was able to hop a fence. This is a tremendous weakness. I'll direct this to Mr. Lord, and if any of the other panel-

ists, although the other three are dealing with Logan here, it's a little different. But this is a tremendous, tremendous weakness we have.

When we had testimony in Homeland Security as the major committee looking back at the Commission reports, we had former Secretary Tom Ridge, and we had the vice chair of that committee, Lee Hamilton, both say that there is a real problem with perimeter security. If we're trying to create uniform standards of security, if we leave that to each local police, when some of these are rural and don't have the resources, you know, with all of the great efforts that you've done here at Logan, if there is a breach in the network, people from here aren't safe.

So my thinking, Mr. Lord, is just it's beyond me not to understand why there isn't some Federal uniform authority over those jurisdictions. Should we be doing that as Congress? I mean, something should be done so that TSA's hands aren't tied, if that's what happened here.

Mr. LORD. Well, actually, I thought Mr. McLaughlin gave a very nice description of the overall who has oversight. Essentially, it's a shared responsibility. Under this current system, a lot of different stakeholders have a role in helping ensure security. I probably know that that doesn't satisfy your question.

But at least, when we looked at this in our perimeter security report, we noticed, first of all, breaches occur on a regular basis. I think there was an average of over 2,000 breaches across the National system on an annual basis. We thought it was important given that the TSA conduct a comprehensive risk assessment to obtain, you know, and to identify vulnerabilities across the Nation and to use that information to better decide what to focus on.

I think the special emphasis reviews Mr. McLaughlin mentioned, that's a good step. That's going to allow them to see, is this a problem on a broader scale or is it unique to Charlotte? So I think they're doing—they're taking the right actions at the moment. I look forward to seeing what the special emphasis review concludes.

But again, you just can't do it on an airport-by-airport basis. You have to do these assessments more broadly. Given the current jurisdiction, everybody seems to have a piece of it, I think that's a good way to proceed. You have to come up with a better visibility on what the problem is on a National scale before attacking the problem.

Mr. KEATING. You know, well, I think the problem is pretty obvious. I think if you are having an investigation on commercial aircraft that are flying all over the country, leaving it to a local police force isn't going to cut it. It just isn't going to cut it. It's an area that we should look at, in my opinion, more strongly.

You know, the whole area of jurisdiction is a problem. As Congress, I must say, at a public hearing just like this, we have our own weaknesses. Because the jurisdiction of homeland security is a patchwork quilt. We're doing our best. I know the Chairman shares my concern as well. We've got to clean up our own jurisdictional problems, you know, for homeland.

But when you're dealing with this and the investigative primary responsibility is in a local airport where, I believe, in that instance—and you're familiar, Mr. McLaughlin—there were sugges-

tions that were a few years old that they just ignored. So you have a situation like this. The locals are in charge, and they're ignoring the Federal Government and their recommendations. So the oversight is important, but it's just not good enough, frankly.

If anyone else wanted to comment on this, I'd welcome any comments.

Mr. MCLAUGHLIN. If I could follow up on that, sir. I would say that, in the Charlotte case, specifically, we do, TSA does have a regulatory authority, and we are able to take certain and significant steps, when necessary. We do still have some open investigations with regard to this case.

But I would point out two specific things, significant things that Charlotte has done in the interim to improve their perimeter securement. No. 1 is, they've increased their police force at the airport by some 21 officers; and No. 2, they've increased their testing, their own internal testing from twice a day to three times a day. So they are taking some significant steps. They've proposed, in addition to that, several changes to their ASP that we currently have for review within TSA and will be responding in the near future on that.

Mr. KEATING. What penalties can you invoke, if they ignore—and I'm not picking on Charlotte. I don't think they're alone. It would be just counterintuitive that this is the only airport that there are problems like this. But you know, this affects all of the folks here, and all of the things we've heard here are undercut when we don't have a uniform, seamless approach to this.

Mr. MCLAUGHLIN. Civil penalties, we would use that mechanism to hold the airports accountable, if they wouldn't comply with our requirements.

Mr. KEATING. Is that fines?

Mr. MCLAUGHLIN. Yes, sir.

Mr. KEATING. Anything else? Do you have the ability to shut down that airport until they get it right?

Mr. MCLAUGHLIN. I would have to get back with you on that answer.

Mr. KEATING. It's an area that I'm going to be looking at myself, because I think we need stronger penalties. They're just ignoring those things, and we cannot have that kind of network across the country.

If I could move a little further, just jumping around. On the SPOT Program and the behavior observation program, I really commend the people here in looking at it and analyzing it.

Could you go into depths about how that analysis is going to occur, and if Mr. Lord or Mr. McLaughlin also have ideas about what should be considered, what kind of metrics are used to evaluate how effective it is and also to make sure, as Mr. Lord said, you know, we can't racially profile people in the United States and we shouldn't.

But when you are doing the analysis, what kind of metrics and safeguards go into making sure that that's not occurring?

Mr. MCLAUGHLIN. I'll take that because it's a National program being conducted here locally.

As I said earlier, the GAO made some strong recommendations with regard to the SPOT Program overall. Many of those have been

incorporated into the assessor or the behavior detection pilot that we're running here in Boston. So we're looking at a broad spectrum of effectiveness, first and foremost security effectiveness. We want to ensure that this is actual working, that it's helping us to mitigate the threat further than what we're doing today.

But second to that, we're looking at the overall impact from an efficiency perspective. So are we ensuring that we're doing this within the constraints of budget and other concerns that we have today. Then finally, we're truly looking at the customer impact. If you have an opportunity to observe that pilot, I would suggest that, in many ways, this enhances the customer experience because it puts TSA in a place where we're having a very human, personal, casual conversation with each customer that approaches us.

So we started the process with baseline data. We had data collectors in Logan evaluating a number of different metrics. Now in the pilot phase, we're evaluating how we're performing against those baseline metrics. Again, they touched the spectrum from effectiveness to efficiency to customer experience. I would be more than happy to set up a briefing where we can go into more detail about what they are specifically.

Mr. KEATING. Thank you.

We're here at the site of the international terminal. I'm curious, in terms of resources, money, and how difficult this is, how do you deal with the foreign language issues when you're having a chat-down? Do you have those resources?

Mr. FRENI. I could speak for Logan Airport. We have many employees, multilingual, that we hire in our public relations and TSR program, public service. Many times, we're called upon to assist with the law enforcement and the TSA to interpret.

Mr. KEATING. One of the things—and you know when we have these hearings, we have to be careful we don't breach any security or give anyone information that we don't want them to have—but one of the things that I'm very curious about, to the extent that you can talk about it, with the new optics program that you are having with MIT and Lincoln Laboratories and Pacific Northwest, with that camera system, it truly is amazing. This is the pilot project that is here, you know, to be tried out here before the rest of the country.

I have an understanding that sometimes, when you look at behavior, sometimes people's actions in a crowd and other things can trigger a computer program where they can zero in on points. That, to me, offers a lot of promise in trying to see, you know, trying to pick out behavior just from an optical standpoint, you know, mechanically.

Is there something that you can, without breaching too much security, is there something that you can inform us about that?

Admiral NACCARA. I can address that. Actually, we considered that, but it's not being deployed at this time. There are a number of problems with that, sir.

No. 1, the angle would be from the ceiling, so you may not have a very good perspective of a person's face. Also, very difficult to read that, and the software has not been proven that good to effectively identify those behaviors in that method.

So at this point, the camera is being used periodically because it requires so much data space just to view the complete terminal, in this case. It's got tremendous acuity and can view numbers on my badge, for example, at the far end of the terminal. It can be programmed to identify or to alarm for certain colors or certain actions. But we do not have the software, at this point, to identify behaviors.

To their credit, MIT is looking at the next iteration of that camera system as well in which they will use many more lenses knitted together to give a 360-degree perspective in a larger area.

Mr. KEATING. Another one of the—oh, I'm sorry. Go ahead, Mr. Lord.

Mr. LORD. I just wanted to note that one of the recommendations in our SPOT report was to better utilize available closed-circuit TVs to refine the program and to help, you know, judge whether you are honing in on the right types of behaviors. So it's good to hear that the TSA is already moving on that.

Mr. KEATING. Did you do any work, Mr. Lord, to see how realistic that might be someday?

Mr. LORD. I know other airports are using more, you know, for lack of better word, hi-def systems. I guess, we were somewhat surprised that every airport has a slightly different approach on the system. We encourage TSA to ensure, you know, that you have a more effective system across all airports. We don't think there should just be this lack of uniformity, which they readily agree with.

Mr. KEATING. I want to give everyone the opportunity to jump in with another issue. But one thing I'll pick up that, again, it's a good opportunity, frankly, to recognize all of the work that the family members of the victims have put into making sure that other people aren't harmed and the work they did with the 9/11 Commission. Certainly, we all feel an obligation as we walk in here every day and remember 9/11 to those family members that we follow through on the hard work of the Commission.

But one of the areas—if I can get some input, it's a great group to ask this question to, I think—one of the weaknesses and the deficiencies that are still there that are identified include the nature of identifications and how they vary from State to State and how they're different.

One of the recommendations that they had is that the Federal Government should set standards for the issuance of birth certificates, you know, birth certificates and all kinds of other sources of identification to make sure that's, well, now you are a major hub, and you are getting people from all States and all countries.

So how can the Federal Government be helpful in setting some kind of uniformity of those identifications?

Mr. MCLAUGHLIN. One thing that we can do and that we're in the process of doing at TSA is developing and deploying software that can read multiple forms of identifications and will apply that against the boarding pass. So that's a new tool that we'll be deploying in the near future that will help us ensure that a proper ID is matched up with a proper boarding pass before we allow access through the checkpoint. I'll defer to others here.

Mr. FRENI. The comment that I'd have from the airline side of the business is that that really needs to be done when the record is developed. Hopefully, there will be some kind of software development where you can pick up on the identification of that person when they make their reservation so it doesn't have to come to the airport to do that.

So hopefully, you know, we can tie that in when someone either goes on-line and makes a reservation and ties it into what we call a P&R system where you'd recognize the identification without any problem and then it avoids the waiting until they get here with their boarding pass.

Mr. KEATING. I'm just probing on areas where we can make changes that have to be made. One of them I think is shameful that hasn't been made by us in Congress and elsewhere is that you meet 8:30 every morning and share information. But when a crisis occurs, that information sharing has to be immediate and it has to be seamless.

Could you tell us, from your vantage point, the importance of having that public safety radio band available, the 10 megahertz that's necessary, so that Nation-wide through all different public safety agencies, you can communicate immediately when something occurs? The fact that that hasn't been done, again, is something I'm just lost at.

I mean, you know, I know there is controversy about, you know, that band. But I honestly feel that's something that should have been done immediately after 9/11. But from your, you know, with boots on the ground, how important it is to have that band, can anyone?

Mr. CONCANNON. I can tell you, sir, that we actually had this conversation yesterday at State police headquarters. There is a strong interest, for obvious reasons. Colonel McGovern, superintendent of the State police, understands the issue. She's been speaking with State officials about the need to have a dedicated band and to have a dedicated interoperability, not just in moments of crisis, but on a daily basis. So it's definitely an interest, significant concern to the State police.

Mr. KEATING. I know, you know, that some of the reviews of 9/11 taught us that so many lives would have been saved had that been in place. Here we are 10 years later, and it's still not in place. So we've got our work cut out for us as well.

People are going to wonder about this—and I'll leave this as a final question that could help us going forward—you know, you've done so much here and you've had innovative programs. They're costly.

Could you comment on some of the means that you use to fund some of the things you've done and some of the needs you have going forward? I'll throw that open to anyone that wants to.

Mr. FRENI. Over the years since 9/11, all of the programs that I outlined in my comments have cost a significant amount of money. We meet with our stakeholders, our airlines, and in some cases, we have to recover those costs through our rates and charges. We do that, and that's the cost of doing business here at Logan Airport.

We've also been very fortunate with our Federal partners to be reimbursed for a good portion of some of the initiatives that we've taken on. One example of that is the inline baggage screening system that we were able to fund and move forward on without Federal funding. We were able to capture a good percentage of that money after we completed it. So we've taken the risk to fund these projects on our own and have tried to find ways through our partners and our users to be able to pay for those initiatives.

Admiral NACCARA. Speaking from the Federal perspective to what Mr. Freni just described, they have been opportunistic at MassPort by being so focused for 10 years, and I'm appreciative of sharing in that embodiment of spirit here.

When they see an opportunity for improvement, they're always leaning forward. When they see that potential, they're exceptionally well-prepared. They will come forward with a very well-justified product, and it's a very compelling argument. When others are still debating whether the concept is fine or should we put money towards that, MassPort will step forward with a quality product that makes it very easy for the Federal Government to say that this is justified. This is the place we should provide some funding. Then everyone benefits in the end.

Mr. KEATING. With the nature of airports, small rural airports, they have unique challenges. I think it's an area where we should continue. Because as I said, one weak link endangers everyone's safety.

So I thank you. I'll yield back my time with that, Mr. Chairman.

Mr. MCCAUL. Thank you, Bill, for that questioning.

I want to thank the witnesses for being here today. This has been a very productive hearing. I also want to thank all of the personnel at Logan Airport that made this hearing possible and the Massachusetts Port Authority and the Massachusetts State Police who are here today for allowing us to host this and for welcoming a Texan to Massachusetts. It's a real honor to be here, and again, thank you for your service. It's been a great hearing.

So I thank the witnesses for their valuable testimony and the Members for their questions.

The Members of the committee may have some additional questions for the witnesses, and we will ask you to respond to these in writing. The hearing record will be held open for 10 days.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 11:17 a.m., the subcommittee was adjourned.]