AIRPORT SECURITY: THE NECESSARY IMPROVEMENTS TO SECURE AMERICA'S AIRPORTS

HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

APRIL 19, 2007

Serial No. 110–25

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE
43–561 PDF WASHINGTON : 2009

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

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California,
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado
VACANCY

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
BOBBY JINDAL, Louisiana
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

SHEILA JACKSON LEE, Texas, *Chairwoman*

EDWARD J. MARKEY, Massachusetts
PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of Columbia
YVETTE D. CLARKE, New York
ED PERLMUTTER, Colorado
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

DANIEL E. LUNGREN, California
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
GUS M. BILIRAKIS, Florida
PETER T. KING, New York *(Ex Officio)*

MATHEW WASHINGTON, *Director*
ERIN DASTE, *Counsel*
NATALIE NIXON, *Deputy Chief Clerk*
COLEY O'BRIEN, *Minority Senior Counsel*

CONTENTS

AIRPORT SECURITY: THE NECESSARY IMPROVEMENTS TO SECURE AMERICA'S AIRPORTS

Thursday, April 19, 2007

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

The subcommittee met, pursuant to call, at 11:37 a.m., in Room 340, Cannon House Office Building, Hon. Sheila Jackson Lee [chairwoman of the subcommittee] presiding.

Present: Representatives Jackson Lee, DeFazio, Clarke, Perlmutter, Lowey, Lungren, Brown-Waite, Bilirakis, and McCarthy.

Ms. JACKSON LEE. [Presiding.] Good morning. The subcommittee will come to order.

The subcommittee is meeting today to receive testimony on the necessary improvements to secure America's airports and what the Department of Homeland Security is doing to protect our nation's airports.

However, before I begin, I would like to ask for unanimous consent that Ms. Lowey, who I know will be joining us, a member of the full committee, be able to sit and question the panel during today's hearing.

Hearing no objection, it is so ordered.

Let me, first of all, thank all of you.

Mr. Lungren, come in. We were just mentioning that you were en route, and we thank the ranking member.

I yield myself 5 minutes for an opening statement.

Let me, first of all, say that we have a bounty of activity today, and because of that, we are told that there may be votes in a short while.

I am going to abbreviate my remarks so at least, Mr. Hawley, we can begin and you may be interrupted during your testimony.

Let me acknowledge the presence of the ranking member, Mr. Lungren, the esteemed distinguished member of the committee, Mr. DeFazio, also subcommittee chair on Transportation and Infrastructure, Mr. Bilirakis, a member of the committee now, Ms. Brown-Waite as well, who is present.

I think it is important to note the philosophy of this committee, and, Congresswoman Lowey, we have already acknowledged, your presence here today, and we thank you so very much for your leadership.

It is very clear that the Homeland Security Committee has one of the most daunting responsibilities in this House. Without any reflection negatively on any other committee, we recognize that as we have looked mourningly at the horrific tragedy of this past Monday, in each of my committees, I have offered to the community of Virginia Tech, the state of Virginia our deepest concern and certainly our respect, our love and recognition of the horror of which they experienced.

But we also know that as time moves on, the questions are asked, "What if?" And this committee would, unfortunately, hold in their hands that one question, "What if?" And so this committee is looking forward, along with a cooperative effort with the Transportation and Infrastructure Committee, close working relationships with the full committee chair and subcommittee chairpersons of a number of subcommittees, to begin to get in front of these many issues.

Today, we will look at a number of security issues. Mr. Hawley we hope that you will provide us with insight on a number of issues. But we certainly are interested in the whole landscape of airports; certainly that of passenger travel and the new technology that we have utilized, but we know the airports are like cities, and, therefore, we are looking at the comings and goings of so many different people.

We need not recount some of our more horrific stories, maybe the shoe bomber, something that we had not heard of before. We knew about airplanes but certainly not passengers with bombs on their feet.

Similarly, we don't know of the comings and goings of the many people that come inside of the airport beyond the area of security. We also know that airplanes and air carriers have to work and function. We need pilots, we need flight attendants. We need to make sure that they get to their planes on time. Probably, we would hear more of an outcry from passengers about late pilots and flight attendants maybe than their own security.

So this committee today is making the statement that we are going forward to take a fine tooth comb, a microscope, if you will, to look at our airports as we look at our rail systems, our mass transits, our critical infrastructure to ensure that we are in fact working together to mitigate, to diminish, to lower the "what if" question.

I think it is important to know that checked baggage is screened for explosives, that it is more likely that the flight has air marshals on board, crew members are trained in defensive measures and some pilots volunteer for the Federal Flight Deck Officer Program to carry firearms to protect the cockpit, some of the things that we have agreed or disagreed on.

We also recognize that it is very clear that TSA has not lived up to its obligation under the Aviation, Transportation and Security Act, which mandates in section 106 improved airport perimeter access security that, "The undersecretary shall require as soon as practical after the date of enactment screening or inspection of all individuals, goods, properties, vehicles and other equipment before entering a secured area of an airport."

VerDate Nov 24 2008 07:47 Jun 15, 2009 Jkt 000000 PO 00000 Frm 00006 Fmt 6633 Sfmt 6633 H:\DOCS\110-HRGS\110-25\43561.TXT HSEC PsN: DIANE

In addition, this section also states that, "The screening or inspection will, at a minimum, be as rigorous as screening of passengers and their baggage."

Certainly, it is unthinkable after 5 years after September 11 a solution as fundamental and simple as this one still has not been implemented, but it is important to note that a meeting with the transportation and security administrator, Mr. Hawley, he has initiated a seven-point initiative that I hope he will explain, which begins to lay a thoughtful concept of beginning to find out who in fact are in America's airports.

So I look forward to the testimony today, and I want us to collectively demonstrate to the nation that we are the committee not of what ifs but how can we and what can we do ahead of time, because we value the security of America every single day that we have the responsibility of that important challenge.

PREPARED OPENING STATEMENT OF THE HONORABLE SHEILA JACKSON LEE, CHAIRWOMAN, SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

I would like to take this opportunity to thank you all for joining us this morning so that we can begin our exploration of the topic of Airport Security and examine what steps we must take to secure the Nation's airports.

In the wake of September 11th, aviation security was made a federal responsibility, and I think everyone here today would agree that aviation security has improved substantially.

Protecting the Nation and shoring up aviation security requires a layered approach.

For example, today, checked baggage is screened for explosives, it is more likely that the flight has air marshals on board, crew members are trained in defensive measures, and some pilots volunteer for the Federal Flight Deck Officer (FFDO) program to carry firearms to protect the cockpit.

However, given the fact that there is an existing threat of liquid explosives, the fact that all passengers names are not checked against the full terrorist watch list, and the fact that we do not screen those who have access to secure areas, it is very clear that TSA has not lived up to its obligation under the Aviation and Transportation Security Act (ATSA, P.L. 107–71) of 2001 mandates in Section 106—"*Improved Airport Perimeter Access Security*". This section states that the Under Secretary—shall require, as soon as practicable after the date of enactment, screening or inspection of all individuals, goods, property, vehicles, and other equipment before entering a secured area of an airport.

In addition this section also states that the screening or inspection will, at minimum, be as rigorous as screening of passengers and their baggage.

It is unthinkable that more than five years after September 11th, a solution as fundamental and simple as this one still has not been implemented. At our nation's airports we meticulously screen passengers and baggage. However, many of the Nation's airport employees and contractors are currently free to roam wherever they want, even in "sterile" areas, without prior screening. Giving workers open access to a "sterile" area is like installing an expensive home security system but leaving your back door wide open.

This is a huge security gap that already has been exploited for the purposes of carrying out criminal activities and I believe that if we continue to use TSA Band-Aid approaches, it is only a matter of time before terrorists exploit this vulnerability to attack our nation.

As Member of Congress and more specifically, as Members of the Committee on Homeland Security, we have a responsibility to make sure our planes and airports are secure. We are at a crossroads—where we must take action to find out what is the best way to provide a safe, secure, and functional aviation system. If we do not put effective, safety measures in place, our Nation may very well be susceptible to another attack, which in turn will cause a major avoidance of commercial aviation. This potential avoidance would subject us to grim economic consequences. We must continually earn the confidence of the flying public. In order to ensure that the public continues to enjoy the freedom of mobility that flying provides, we must demonstrate to them that our Nation's airports are secure.

Ms. JACKSON LEE. It is now my honor to recognize the ranking member of the subcommittee, the gentleman from California, for an opening statement for 5 minutes.

Mr. LUNGREN. I thank the gentlelady for the time, I thank the other members for their attendance, and I thank our witnesses for being here.

We know that we have done a lot of work in the area of aviation safety and security, and we know that that has made us much safer than we were on 9/10 or 9/11, but we also know that much more remains to be done. And there has been the interest of members in particular of this committee about the question of security with respect to those employees who have access to otherwise secure parts of the airports.

And there has been a debate about a perimeter defense, if you will. I look forward to hearing from Mr. Hawley about that approach versus the new initiative that he is announcing, how they might differ, how they might have aspects of separation that may make some airports more conducive to one approach and other airports conducive to another.

I also believe that it is important for us to have pilot projects to go forward so we can have some comparisons and also so that we can move forward rather than just talk about it.

And, lastly, I would just like to mention that, as Mr. Hawley knows, there has been a concerted interest on this committee for the effective use of canine units, the ability that they have to supply your department with an agility that they might otherwise not have and that that may answer some of the questions with respect to construction concerns that we have that confront us when we are dealing with machines of technology.

So I look very much forward to hearing the testimony of our witnesses today about what they believe is the best approach for eliminating the threat that may be posed by airline employees.

Let's say, for the record, most of the airline employees do an outstanding job, are loyal Americans, but what we are looking at are potential vulnerabilities and how we avoid those vulnerabilities.

And with that, Madam Chair, I would yield back the balance of my time.

Ms. JACKSON LEE. I thank the distinguished ranking member.

Let me acknowledge the presence of Mr. McCarthy as well. Welcome.

And let me ask unanimous consent to yield to the gentlelady from New York 30 seconds.

Mrs. LOWEY. Thank you very much, and I wanted to thank the subcommittee chair, Ms. Jackson Lee, and the ranking member, Mr. Lungren, and Chairman Thompson and Ranking Member King for allowing me to participate in this critically important hearing.

I look forward to working with each of you to advance my legislation to initiative a pilot program for screening airport workers and to take additional steps toward achieving total 100 percent screening at U.S. airports.

Additionally, I want to thank Assistant Secretary Hawley for the frank discussion we had yesterday afternoon. I know we don't agree, we don't see eye to eye on which strategies would be most

VerDate Nov 24 2008 07:47 Jun 15, 2009 Jkt 000000 PO 00000 Frm 00008 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-25\43561.TXT HSEC PsN: DIANE

effective, but I did appreciate the opportunity to continue having an open and frank dialogue with you of the issue.

And I do want to thank Ms. Brown-Waite for being an active cosponsor of this legislation.

Thank you very much. We look forward to the hearing.

Ms. JACKSON LEE. I thank the gentlelady.

At this time, I would like to welcome Kip Hawley, the assistant secretary of the Transportation Security Administration at the Department of Home Security, and I would correct that and say he is an assistant secretary of Department of Homeland Security and administrator for the Texas—Texas on my mind—Transportation Security Administration.

You know what happens when you come from a big state.

I want to say to you, as Congressman Lowey has said, overall, I think it is a good tension between this committee and the Department of Homeland Security in terms of oversight. We don't always agree, but let me acknowledge that you have been a wonderful breath of fresh air with respect to the dialogue and the interest that you have had in working with Congress on this very large challenge that we have. We are delighted of the new attitude, and we certainly welcome you to this committee.

Might I say that, without objection, Administrator Hawley's full statement will be inserted into the record.

And now I ask that you summarize your statement for 5 minutes. And thank you for being here.

STATEMENT OF HON. KIP HAWLEY, ASSISTANT SECRETARY, TRANSPORTATION SECURITY ADMINISTRATION

Mr. HAWLEY. Thank you. Thank you for those kinds words.

Good morning, Madam Chairman, Mr. Lungren and members of the committee. Thank you for this opportunity to discuss security at America's airports, as you prepare to mark up legislation in this area.

We generally look at aviation one slice at a time. We look at what do we do for employee screening, for air cargo, for passenger checkpoint baggage, perimeter security, one by one. But it is very, very important that we keep in mind that to terrorists we are one target, and they don't care which particular place they attack.

So we need balance and flexibility in all of our security measures. If we jump from concern to concern, mandating measures for each one, we may tie up critical resources that do nothing more than make it easy for a terrorist to attack somewhere else.

If an attack is successful, it does us no good to say that we were impenetrable at a different spot.

I will outline for you this morning TSA's plan for effective screening of airport employees. It is, in my view, the most effective security for this environment.

Passenger screening uses a different model than airport employee screening, and it makes common sense that we use a different approach. Passengers come to the airport, and not much is known about them. We move them through security and hold them in a sterile area before they board the plane.

It is a completely different thing with airport workers. We know a lot about them, and they are well-known to each other. When

VerDate Nov 24 2008 07:47 Jun 15, 2009 Jkt 000000 PO 00000 Frm 00009 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-25\43561.TXT HSEC PsN: DIANE

they come to work, they are gaining access to the equivalent of a small city, which already contains more than enough raw materials to commit a terrorist act.

Therefore, keeping track of people and what they are doing is a better approach to security. It doesn't make sense to dig in security resources, looking in lunch pails when the real vulnerability is what happens inside the airport property.

Magnetometers cannot detect suspicious behavior. In fact, installing fixed checkpoints makes the job easier for terrorists. Although it may be comforting for us to see employees in line for screening, a checkpoint provides an unchanging, predictable barrier that sits in one place every day. The terrorist can spend all the time he or she needs to find ways around, over or through that checkpoint.

For this reason, we must use many layers of security, each one nimble, unpredictable and dynamic. And just as we are pushing the perimeter of security past the checkpoint for passengers with behavior observation, document checkers, canine, things like that, we are using the same strategy when it comes to employee screening. This leads me to the plan I am here today to discuss.

With our airport partners, including airport law enforcement, we have agreed to create a practical, workable solution to employee screening. It is an evolution on top of what we do today and adds real risk-based security.

TSA already has a layered approach in place for the nation's airport workers, and I have outlined that in my prepared statement; be happy to talk about it.

But here is what we are adding on top of it, a six-point security plan for employee screening as follows. Number one, behavior observation. The population of highly skilled officers will grow beyond TSA to include airport employees trained to recognize hostile intent and suspicious behavior.

Second, employee training on top of what they receive already will raise awareness of suspicious behavior and what to do about it when you find it.

Three, targeted physical inspection. We will now add airport employee to roving patrols to TSA's random, unpredictable employee screening. That is on top of everything we do in the random sector. This adds additional physical security screening, including at the point when they come to work.

Fourth, biometric access control. This will add security by knowing who is where in the airport.

Fifth, certified employees will create a new level of employee risk assessment that will allow established low-risk employees easier mobility to do their jobs.

And, finally, the technology component where security technology will continue to be deployed and developed for specific use in the airport environment, add things like cameras and not necessarily new things that have to come out of R&D but an integrated use of cameras can have tremendous security effect.

Better overall security is achieved if personnel are not tied down to checkpoints, checking and rechecking people that work in the airport every day. We want our security resources on the move so

that terrorists cannot plan an attack knowing what defenses they will face.

I appreciate the committee's interest in working with us on a pilot approach to further explore the options, and we will be good partners in the effort. And I see a lot of common ground with where we want to go, and the pilots will be a good way for us to establish further data to move forward.

We don't need, however, to wait to implement what I just outlined. We have already begun to work to start implementation.

So thank you for your time and attention. I would be happy to answer your questions.

[The statement of Mr. Hawley follows:]

PREPARED STATEMENT OF THE HONORABLE KIP HAWLEY, ASSISTANT SECRETARY, TRANSPORTATION SECURITY ADMINISTRATION

Good morning, Chairwoman Jackson-Lee, Ranking Member Lungren and members of the subcommittee. I am pleased to appear before you today to discuss airport security.

At every airport security requires partnerships. TSA, airlines, airports, law enforcement and passengers must work together. Only through cooperative partnerships are we able to provide a robust security system. But airport security is only one layer of security in a larger security system whose mission is to reduce the risk of emerging threats to the entire transportation system.

Aviation security begins well before a passenger arrives at the airport.

1. U.S. government agencies work with others around the globe to identify and disrupt terrorist activities at their source.
2. Customs and Border Protection activities further identify potential terrorists and bar their entry into the United States.
3. Federal, State, and local law enforcement work together with the FBI in Joint Terrorism Task Forces across the United States to identify and disrupt terrorist activities within the U.S.
4. A No-Fly system is used to prevent anyone known to an agency of the U.S. government to be a threat to commit a terrorist act from flying into or in the United States.
5. Airline flight crews and airport employees who have access to an aircraft are subject to an even stricter vetting standard than the No-Fly analysis.

These first five security elements mean that anybody known to U.S. intelligence or law enforcement agencies as a terrorist or a close terrorist associate never gets close to an airplane. But there is much more.

6. An additional, risk-based computer-assisted pre-screening of passengers is conducted before a boarding pass is issued.
7. Hundreds of canine teams and local law enforcement officers are working at airports across the country to identify suspicious articles or people.
8. Surveillance activities take place in and around the airport environment on a daily basis. In 31 airports today, specially trained Behavior Detection Officers look for suspicious behavior.

All of this happens before a passenger even shows up at a TSA checkpoint.

9. At the checkpoint, a professional, well-trained, experienced team of Transportation Security Officers (TSO), assisted by multiple technologies, screens passengers and their carry-on bags for weapons and explosives.
10. In the baggage area, similarly well-trained, experienced Transportation Security Officers use a variety of technologies to screen baggage, and, when necessary, they physically search baggage to resolve anomalies.

Then, on the aircraft:

11. Thousands of Federal Air Marshals fly undercover on a very significant number of flights, both domestic and international.
12. Thousands of pilots who undergo special training and become Federal Flight Deck Officers are authorized and ready to protect the cockpit with firearms.
13. Other local, State, and Federal law enforcement officers travel armed as part of their normal duties and are prepared to intervene.
14. Hardened cockpit doors prevent unauthorized access to the flight deck.
15. And sitting on every airplane are passengers who remember the courage and commitment of the men and women on United Flight 93, and who are prepared to act, if necessary.

Each and every one of these 15 security layers is important.

Relying solely on security at the checkpoint or focusing all of our resources to defeat one threat is counterproductive and detracts from our overall mission. The 9/11 Commission recommended a layered security system saying: "No single security measure is foolproof. Accordingly, the TSA must have multiple layers of security in place to defeat the more plausible and dangerous forms of attack against public transportation." (p.392).

Control of access to sterile and secured areas is just one of the many aviation security layers we have in place. We recognize that, despite our efforts to make each layer as strong as possible, a concerted effort directed at any one layer could be successful. But there is tremendous power in the reinforced, multiple layers. Truly, the whole is greater than the sum of the parts—and, together, they are formidable.

This plan is more rigorous than 100 percent machine screening of employees at a stationary checkpoint. Because airport employees move about the facility and are not confined to a sterile area (as are passengers), they have access to items throughout the airport and to items introduced at the perimeter. The idea is not to check all employees at specific, known locations, but to check them throughout the facility, to discern hostile intent, to track their movement patterns, and to train employees to detect suspicious behavior. An added dimension of this plan is to narrow the field of employees that we need to know more about on a regular basis. We can do this by creating a level of "certified employees" who have been subjected to a more rigorous, initial level of scrutiny on a voluntary basis and remove them from the regular, but not random screening regimen.

Employee Background Screening

Today, someone working in a sensitive airport environment undergoes extensive review before being allowed unescorted access. Airports must submit fingerprints for each individual who is employed or performs duties in the Security Identification Display Area (SIDA) or the sterile area at our Nation's airports. The fingerprints are used to conduct a criminal history records check to ensure that the airport does not grant unescorted access to individuals whose background reveals a disqualifying criminal offense. TSA also conducts name-based security threat assessments of the name against its terrorism and other Federal databases of these individuals as well as anyone with an airport-issued identification medium that allows access to these areas. Any name that is a possible match to a database is referred to appropriate law enforcement or intelligence agencies to determine whether the individual's identity can be verified, and whether the individual continues to pose a threat. TSA informs airlines or airports if an individual's access to secure areas must be denied or rescinded. TSA will soon increase the scope of the Security Threat Assessments to include any individual who holds or is applying for airport-issued personnel identification medium. The Security Threat Assessments of all identification medium holders are conducted on a perpetual basis.

Generally, in order to access sterile or secured areas, anyone who has not been issued a Security Identification Display Area (SIDA) badge for a particular airport, including airport and airline personnel, vendors and contractors, and even TSA employees, must pass through the TSA security screening checkpoint and submit to the same physical screening process that passengers must pass through before boarding an aircraft.

Airport operators are responsible for developing and implementing TSA-approved airport security programs procedures and processes to control access to sterile, secure and SIDA areas. These programs must include badging, a challenge program, and a compliance regime. All entrances must be secured, and this is generally accomplished by guards or with electronically controlled locks. Nearly 1,000 TSA Aviation Security Inspectors ensure that airports and air carriers comply with the regulatory requirements. In addition, although individuals with a SIDA badge are not required to pass through a screening checkpoint in order to access SIDA areas, TSA, for some time now, has been conducting physical screening of individuals and vehicles entering SIDA areas on an unpredictable basis at numerous airports.

By building unpredictability into our screening and oversight operations, deploying new technology as it becomes available, and utilizing all of our resources more flexibly, we can continue to improve the formidable system of layered security that now exists.

Aviation Direct Access Screening Program (ADASP)

In July, 2006, TSA implemented the first version of the ADASP that requires screening of airport employees, their accessible property and vehicles upon entering a direct access point screening location for identification, prohibited items and items of interest. Again, while I cannot discuss all of the operational details of ADASP in this setting, I can tell you that the program emphasizes the random and unpre-

dictable aspect of our approach to security. Its scope can take in all or some components of airport security to include gate screening, SIDA identification, cargo or the aircraft itself. Its specific focus, location and duration remain dynamic. It may also include assisting airport and aircraft operators in the performance of their security responsibilities. With our current personnel policies, we are able to surge these activities, as in Orlando, on very little notice.

Recent Incident at Orlando

On March 5, 2007, TSA ordered a Delta flight from Orlando to San Juan to be reverse-screened upon arrival, based on information that there were potentially weapons onboard the aircraft. An individual carrying 14 weapons and eight pounds of marijuana was apprehended upon deplaning in Puerto Rico. TSA coordinated efforts between Orlando and San Juan that included local police in both jurisdictions and the FBI. Because an investigation is still ongoing, there is a limit to what I can say in this setting.

The incident, however, raised regional and national awareness of the employee "insider threat" at our nation's airports. TSA quickly deployed more than 160 transportation security officers, aviation security inspectors, Federal Air Marshals and other personnel to augment already existing employee and passenger security efforts.

Shared Responsibility

TSA recently expanded its ADASP through Saturation Security Teams (SST) at airports in the region including Orlando, Miami, Fort Lauderdale, Tampa and San Juan. In addition to ADASP, the teams employed behavioral observation techniques, aviation security inspections and other demonstrations of random-continuous security. This operation was marked by a sharp increase in random, unpredictable screening of employees in secure areas. Access to secure areas was limited during non-business hours and door access during those hours was audited for suspicious activity. We deployed integrated teams of Federal Air Marshals, K–9 teams, law enforcement officers and transportation security officers to areas throughout the airport. We conducted random screening of employees and passengers at boarding gates, including using behavior observation techniques, and we randomly inspected aircraft.

The recent surge illustrated TSA's ability to implement random, unpredictable security enhancements anywhere in the nation on short notice. Surges are now a permanent part of our security posture and could occur anywhere, at any time, as part of our unpredictable approach.

This mobilization illustrates TSA's ability to quickly and unpredictably deploy assets based on risk. The agency has developed a longer-term, sustainable plan with our airport and airline partners not only for the Florida/Puerto Rico region, but for the entire U.S. aviation system. TSA will conduct additional operations in other regions in the coming weeks and months on an unannounced basis. Finally, with regard to TSA's workforce at Orlando, several new measures have been established that will further tighten security at Orlando.

At the request of Greater Orlando Airport Authority (GOAA), TSA has entered into a 90- day agreement to take over employee screening at the SIDA access doors in the passenger terminal in exchange for GOAA taking over non-security functions that TSA previously provided. Additionally, GOAA has entered into a contract with a private provider to conduct employee screening at the vehicle checkpoints. While TSA advocates a multi-layered approach to security, we are willing to assist our airport partners in Orlando to meet their goal on a short-term basis. Because of the airport's limited number of employee access doors and willingness to provide personnel to conduct non-security functions, TSA is able to come to this agreement without negatively impacting security in other areas or wait times.

Conclusion

Over committing TSA resources to inflexible, resource-intensive measures is not consistent with our risk-based approach to aviation security. TSA moves resources in a flexible, unpredictable fashion to address both known and unknown threats with a layered security approach.

Airports have primary responsibility for employee screening, with TSA acting as a regulatory authority. This operation, as well as the broader ADASP program, augments airport security already in place.

TSA employs a risk-based approach to security, including roving transportation security officers that search employees, their packages and their vehicles. Every employee should have a reasonable expectation that they could be screened at any time, at any access point within the footprint of the airport. That applies to all airports, not just where a surge is occurring.

I am aware of Representative Nita Lowey's introduction of HR 1413 as well as HR 1690 to require pilot programs for physical screening of airport workers with access to secured and sterile areas of airports. I look forward to working with Representative Lowey and the Subcommittee on this very important issue.

By building unpredictability into our screening and oversight operations, deploying new technology as it becomes available, and utilizing all of our resources more flexibly, we can continue to improve the formidable system of layered security that now exists.

Ms. Chairwoman, thank you again for the opportunity to testify today. I would be happy to respond to questions.

Ms. JACKSON LEE. Thank you very much.

At this time, I would like to remind each member that he or she will have 5 minutes to question Assistant Secretary Hawley.

And I thank him for his insightful testimony.

And I will now yield myself 5 minutes for questions.

I said earlier that many times we have moments of agreement and many times moments of disagreement. I, frankly, think that it was important for you to make this announcement. I think also the committee believes that it is long overdue and, frankly, should have been done more than a number of years ago.

So in my first question, or a series of questions, I will ask two together, is for you to give me a sense of urgency to complete these elements but more importantly then to move to next steps. And, as you well know, there is underlying legislation that we will be looking at, as well as a number of amendments on the question of who is at our nation's airports and how are they documented.

Then I would like you to answer a more specific question that I think gives us a sense of the problem, and that, of course, the issue at Orlando International Airport that happened with the Comair employees and those who, I think, were able to game the system. How long did they exploit the breach and what exactly happened?

Mr. HAWLEY. I will take them in order of pace.

We agree with you on the urgency of it, and since the August liquids threat when the airports really were able to help us—and airlines—stand up a totally new security regime overnight, we did that in August and have been sustaining at a very high level of alert, including at the orange level, which requires significant additional activity by airports.

And as we have been discussing how we can make those measures sustainable if we have to keep it orange, we have been developing solutions together to increase the security and be able to sustain at that high level. So that is really the genesis of what I am talking about, and it is with a great deal of urgency that we get after it, because we do recognize the possibility for someone trying to use employees.

Now, on the Orlando incident, specifically, I can't get into the exact details of that, because that is an ongoing active investigation, but it does raise the issue of who are these people working at our airports, how much do we know about them, what security is there?

So, in general, without specific to that exact thing, one of the learnings from that involves—when I said knowing who is at the airport, we already do know that, because we do all the background checks, and we keep track of them with their badge, but knowing where they are at the time, this is an additional way to get at it.

So if somebody is normally supposed to be in one place and shows up in another, there is a good opportunity, if we can capture that and address it at—

Ms. JACKSON LEE. Have you discovered how long the breach was going on?

Mr. HAWLEY. Well, that is subject to an FBI investigation, and I think in a non-public setting we or the FBI could give you the full story.

But mentioning the FBI, it is also important to note that their joint terrorism task forces are extremely active and include the airport jurisdiction. So in addition to everything TSA does, the FBI joint terrorism task forces are all over what is going on at airports. And if there is the first sniff of anything involving something with terrorists, that is a red hot thing that we all get on.

Ms. JACKSON LEE. But you can understand our concern, Assistant Secretary, when—and you are right, we will have a further classified briefing, but you can understand the public statement is that there has been a breach. We don't know how long that breach has occurred. We don't know whether there are many breaches going across America's airports. And, therefore, it is more than a sense of urgency that we have standards, regulations, enforcement.

And so someone might think whether or not the announcement yesterday would have anything to do with the fact that there are potential legislative initiatives being acted upon.

Mr. HAWLEY. I think we are grateful for the public attention on the issue that this brings, and it is taking an opportunity to get the public focused on it and to say, "Yes, these are things that we are doing on top of the other measures."

But we have an ongoing, it is an evolution, we will never finish adding security to the system and finding better, more practical ways to get it done.

Ms. JACKSON LEE. So you are not intending to put an undermine under the legislative initiative going forward.

Mr. HAWLEY. No. No. I think, frankly, this is baseline thing, and it is, I believe, completely compatible with Mrs. Lowey's bill on the pilots. We can work with the committee to agree on a series of pilots.

Ms. JACKSON LEE. There are so many bells.

Let me thank you for your testimony, and let me now yield 5 minutes to the distinguished ranking member.

Mr. LUNGREN. I think I know what we are going to be doing in a few minutes.

Thank you very much for your testimony, Mr. Hawley.

Six-point plan, how soon is that going to be actually implemented?

Mr. HAWLEY. The elements regarding training, we are working on now to define exactly what that training is. We have got the training for our TSOs and now to package it for use for airport environment will not be a difficult thing. The airports already do a lot of training. So I think that is the first one out. I would be looking in the 3-month range to get that going.

The most longer-term one would be the biometrics. So I think in this year we will have the standards or a concept of operations, how that will come into place.

Mr. LUNGREN. And I know you touched upon this in your testimony but I wish you had elicited a little bit more on the challenge that you have for securing the entire airport environment with respect to employees that may be moving around and I think, as you mentioned, their ability, once they gain access to the airport to find things that taken together or even individually could be used as weapons or cause destruction of a damaging nature.

And you talked about the multilayered approach, but what I am trying to get at is how do we as a committee come up with legislation that directs you to do what I think you know we want to done but gives you the flexibility so that it can actually be accomplished with the reality of the different type of airports we have here? And how do we do that so it doesn't look like we are giving you a hedge so that you are not doing what we are actually asking you to do?

Mr. HAWLEY. Yes. I think the experience we have had working with air cargo is a good example where we started off in different places but wanted to get to the same security result. And I think as we have worked along over the last couple of months, that figuring a way to make it operationally feasible to get the very thorough screening for air cargo is a good way to look at this.

And I think we can do the same thing here through the pilots. We want to get to the same result that the committee wants to and Mrs. Lowey wants to do in terms of measurable risk reduction in that environment.

So by doing these pilots, I think that is a good way to do it, and then just continue to work together to make things operational, like the standard of passenger screening doesn't make sense in the backside of the airport where we have tens of millions of gallons of jet fuel and blow torches, and so for us to be confiscating lighters from workers coming in is not something that I think any of us would say that is a good idea.

So we need to look at the actual specific of what the measure is and not tie us down and make it operationally infeasible. But we are willing to try very innovative things to achieve the result.

Mr. LUNGREN. And the use of canines in this whole operation.

Mr. HAWLEY. Very key part for the whole thing, because canines can work anywhere in the airport environment. Again, it is a wide variety of threats. Very good deterrent, very good effective bomb detection, and we are very enthusiastic about the canine program.

Mr. LUNGREN. I mean, you are enthusiastic about it, but where are we in terms of number of teams necessary to do the job? Because this is something Mr. Pearce started us looking at a year or 2 years ago when he was on the committee. And there was some concern that while we need to pursue the technology fixes and the new machines and try and get the best technology in place, we might not be putting enough emphasis and enough money behind sufficient number of canine teams with the adaptability that they possess to do the various jobs that are necessary.

Mr. HAWLEY. We are somewhere short of 400 dog teams, and we continue to grow that. This is—

Mr. LUNGREN. You are not saying you are short 400 dog teams, you are saying you are just slightly less than 400.

Mr. HAWLEY. Yes. Yes. I will have to get the exact number for the record, but it is around 400. It varies because we are kicking

out new teams frequently. We are also putting them in the transit environment., so we use some of our dogs to go to transit. But we agree on that strategy of brining in dogs right now while we develop long-term technology.

Mr. LUNGREN. Thank you.

Mrs. LOWEY. [Presiding.] Just in case there is a little confusion, the chair and Mr. DeFazio went to vote, so I am asking a question. Then we are going to recess, I gather, while we all vote and then come back. So I will be quick here.

Mr. LUNGREN. So non-members of the subcommittee can be chair? Can I be the majority for the day?

[Laughter.]

Mrs. LOWEY. I don't know.

Okay. We will move quickly before you check that in the room.

[Laughter.]

Mr. LUNGREN. I reserve my objection.

Mrs. LOWEY. Thank you very much.

If I can get through a couple of questions quickly, and then we will adjourn and go and vote.

Does TSA have the screener and technology resources necessary to conduct 100 percent employee screening?

Mr. HAWLEY. Not at the same level as passenger screening, no. It would almost double our total number of people screened.

Mrs. LOWEY. So at some point, I think it would be helpful to know specific numbers and what it would take to do it. Because it is always blown up, and there are all kinds of rationale, as you know, because you presented the rationale to me, but we never really get the accurate statistics. So we will follow up with you on that.

Mr. HAWLEY. Yes, ma'am.

Mrs. LOWEY. Has TSA revised its screener allocation model to account for the additional duties required of screeners, such as randomly screening employees?

Mr. HAWLEY. Yes, that is incorporated into our staffing model.

Mrs. LOWEY. Now, several airports report that TSA does not have adequate staffing to efficiently and effectively screen passengers, baggage employees, aircraft under the Aviation Direct Access Screening Program. And with the busy summer schedule fast approaching and the additional duties required of screeners, how will TSA ensure that passengers and baggage are processed in a timely manner while preserving a high level of security?

Mr. HAWLEY. Every manager I have ever worked with didn't have enough resources, and I think that is true with our guys. We have run the numbers, and we are flexible on how we do the ADASP program. And I believe just like last year we will handle the passenger load effectively.

Mrs. LOWEY. Have you consulted with both airports and airlines in the development of your employee screening program?

Mr. HAWLEY. Yes.

Mrs. LOWEY. Now, I understand that TSA has proposed a layered approach to enhancing airline-airport employee screening that includes targeted physical inspections, increased training on how to recognize suspicious behavior, monitoring of employee access points with cameras. Why do you think—you didn't convince me yester-

day—so why do you think that approach is better than 100 percent physical screening by magnetometers?

Mr. HAWLEY. Because if the screening by magnetometers is at the perimeter, as you mentioned, the resource to get at that screening would make it harder to do the screening on the inside of the airport, which is where the action is. And being unpredictable everywhere on the airport is something that is a far better security measure than saying once you break through the checkpoint on the outside, you have free reign of the whole city.

Mrs. LOWEY. Well, had the new policy that was announced yesterday been in place in Orlando at the beginning of March, would that have prevented the two individuals from boarding a plane with a bag full of firearms and narcotics?

Mr. HAWLEY. I am not going to talk about that specific event, although I believe history will show there was no threat of a terrorist event on that particular flight, although it does raise valid issues about employee access.

Mrs. LOWEY. Okay. Now, wouldn't 100 percent physical screening have prevented the incident?

Mr. HAWLEY. I can't talk about the actual operational details of that area. I would point out that guns and drugs are not unusual in the airport environment, and throwing things over fences and finding other ways than going through checkpoints is a possibility.

Mrs. LOWEY. However, if those workers had gone through a metal detector, would it not have detected what they were carrying?

Mr. HAWLEY. They would have, I believe, the same result, because they did go through metal detectors. They just got their guns in a different way. So I don't dispute that adding additional screening on the outside can be very good for security. It just can't be a static measure that ties up all of your activity. It is a part of the puzzle, not the complete security.

I would say from a real security point of view, keeping track of what is going on on the inside of the perimeter is of higher security value than magnetometers on the outside.

Mrs. LOWEY. I am a little confused here. You are talking about other ways to detect it. If there are guns hanging around the airport in a drug store or at a food store, we have real problems here. So you are saying that they could have gotten the guns in another way, and if we had a system whereby every worker had to go through a metal detector, they still could have gotten the guns in? Maybe we have to do a regular search of all the various booths or stores at the airport.

Mr. HAWLEY. That is why the key thing is the people, because there are, in the normal course of business, all of the things you would use for a terrorist incident, including guns, in the normal course of business in the airport. So the trick is, yes, try to keep them out, but also know who those people are and keep an eye on them when they are inside.

Mrs. LOWEY. Well, I agree we have to do everything. The 5 minutes is up. We have to vote. My 5 minutes is up.

I must say, you are a persuasive gentleman, but you haven't convinced me that it doesn't make absolute sense to have every worker go through a metal detector. At least you are decreasing the odds.

So I know we will have further discussion on this, and I would appreciate any additional information about cost, et cetera, because I feel when we are spending billions of dollars on our defense of our country when we are spending billions of dollars in Iraq, this is essential.

So I thank you very much for appearing before us.

The committee stands in recess.

[Recess.]

Ms. JACKSON LEE. [Presiding.] We will re-begin the hearing.

And I would like to yield 5 minutes to the distinguished gentleman from Oregon, former subcommittee chair to the Committee on Aviation for Transportation and Infrastructure, Mr. DeFazio.

Mr. DEFAZIO. I thank the gentlelady for the time and for her leadership on this and other important homeland security issues.

I guess, Mr. Hawley, I would like to ask what is proposed in terms of a pilot. Do we have, essentially, an ongoing pilot in Miami Airport? My understanding is they are screening all employees there.

Mr. HAWLEY. I think we have functionally an ongoing pilot, and I believe in the next panel you will hear from Miami Airport, but it is a very good program.

And I think one of the significant pieces about it that I view most effective is the behavioral observation training that the airport, in conjunction with Miami Police Department, has gone with for the employees. And that adds very significant security beyond whatever airport screening they do.

Mr. DEFAZIO. This is sort of the neighborhood watch aspect of what you are proposing that TSA would adopt as a nationwide policy. And that is essentially, sort of, modeled a bit on what we are doing in GA, right, where we have, essentially, the Airport Watch Program?

Mr. HAWLEY. Yes. The way I look at it, in a passenger environment, just think as if everybody on the plane flew the same flight every day with the same people. You get to know who belongs, who doesn't, what they are doing is normal or not. If we give them an avenue to relay that information, that is a huge security value.

Mr. DEFAZIO. Right. Just for a moment, it is not on the topic, but the GA Program, are we funding that? I mean, it is very modest cost. Is that in the budget?

Mr. HAWLEY. Well, the industry has taken that on and essentially does that themselves.

Mr. DEFAZIO. I thought there had been some apportionment.

Mr. HAWLEY. Well, I am sure there is a small amount of money, but—

Mr. DEFAZIO. Okay.

Mr. HAWLEY. —but I think it would not be fair to say that we fund that.

Mr. DEFAZIO. No, no, but I thought that there was some contribution, that is all.

So but as you are anticipating this, sort of, program in the airports, TSA would perform the training or you would contract for the training and those sorts of things, you would have roving security teams, as I understand it. Do you envision trying to move more people through security also?

Mr. HAWLEY. I would definitely have the effect of screening more people. With our own program that we do with our transportation security officers, it is not trivial. It is on the order of 4 or 5 or more hours a day at airports across the country. So that is a significant piece of screening that goes on in various places around the airport. Adding to that would be a different program operated, for instance, by the airport to do the same kind of thing.

Mr. DEFAZIO. And then just on the issue of if we were to move toward full screening of all employees and everything coming in the backside of the airport, do you have a cost estimate on that?

Mr. HAWLEY. We have looked at that, and the number of people—about 800,000 people have SITA badges, and they go through frequently during the day. So if you just roughly double it, that is only twice a day, that is equivalent to what we do today.

I think, in a practical sense, we would not go with passenger screening, as I mentioned, the lighter thing or take away tools. You can't take away tools more than 7 inches for airport workers. So there is some accommodation that will need to be made for practicality, and that would cut the cost down somewhat. So that is the detail. How many checkpoints you do, are you doing a ballpark look in the bag or how much are you going through the bag and examining each item? That will define the cost, and I think the pilots give us an opportunity to really field test what it does cost.

Mr. DEFAZIO. What size airport would you recommend for a pilot?

Mr. HAWLEY. I think, as Mrs. Lowey's bill includes, it talks about all sizes. Because, as you know, each airport is different, and each size airport has different things. And as you also know, at the very small airports, they don't have SITA badges, so you have to figure out what is the practical way of doing it. But at a small airport, everybody really does know everybody else.

Mr. DEFAZIO. Now, as far as I know from our past conversations, in fact, I believe in a recent hearing or meeting, I can't remember, oh, briefing perhaps, we seem to see you a lot these days, TSA is asking this year that an additional 1,600 employees be in the budget; is that correct?

Mr. HAWLEY. Yes, sir, for document checking purposes.

Mr. DEFAZIO. Right. So you are, at the moment, if you had additional staff allowance or funding, your highest priority would be the document checkers.

Mr. HAWLEY. That is correct.

Mr. DEFAZIO. Where would you put—and maybe you don't want to say this in a public setting—never mind, I won't even ask that question.

But let me point to the, kind of, obvious, I mean, what happened at Orlando. Is what you have proposed, I mean, what likelihood do you think that what you are proposing would have prevented that kind of penetration and problem?

Mr. HAWLEY. Well, I am trying to figure out a way to give you the answer to your question without getting improperly into to the specifics. But I can say this, that we have looked very, very, very carefully at that as a learning experience, and we have taken whatever learnings are appropriate and incorporated them in our own practices as well as in some of things here. So I think although the

specifics of that one I don't want to talk about, they do highlight the opportunity for inside employees to be turned against the system, and it is a serious thing we have to pay attention to.

Mr. DEFAZIO. And then you also mentioned—just one last quick thing—cameras. I just had a recent visit at San Francisco, and they have an extraordinary system of cameras throughout and around the airport.

Mr. HAWLEY. I think that is exactly what we are talking about.

Mr. DEFAZIO. Okay. Thank you.

Thank you, Madam Chair.

Ms. JACKSON LEE. Thank you very much.

Let me remind members that I will recognize members who were present at the start of the hearing based on the seniority on the subcommittee, alternating between majority and minority. Those members coming in later will be recognized in order of their arrival.

Might I now yield to the distinguished gentlelady from Florida, Ms. Ginny Brown-Waite, for 5 minutes.

Ms. BROWN-WAITE. I thank the chairwoman for acknowledging me.

And thank you, Mr. Hawley for being here.

When I read over your testimony last night, I was absolutely shocked that you would say that the Orlando incident raised everyone's awareness.

Sir, with all due respect, Nita Lowey and I and other members of this committee have been saying, "There is a serious problem here at the backdoor of the airport." Actually, it was a TSA employee who tipped me off to this.

Let me ask you this: When TSA employees report to work, do they have to go through the initial metal detector screening every day?

Mr. HAWLEY. Yes.

Ms. BROWN-WAITE. Do you not think that these are people who have been vetted, who have had their background checks done, who have certainly a higher level of security than perhaps someone who is on the cleaning crew or working at a restaurant? It flies in the face of what Americans believe security should be to know that the person who is checking them gets checked, but the backdoor people just come in with a little magnetic card. And so for you to say that America's awareness and the agency's awareness—

Mr. HAWLEY. No, no. I did not say the agency's awareness. You will note in our ADASP Program was rolled out in June, and since I came to this agency, we went right after issues that are beyond the checkpoint, IEDs, we have been all over this, and I have had conversations, frankly, with Mrs. Lowey right from the start, and our program is now extremely sophisticated. As I mentioned, we have hundreds and hundreds of our TSOs working on these backdoor things, and they have been going on since last summer.

Ms. BROWN-WAITE. Have you considered, perhaps, having the vendors add another nickel to the already unhealthy corndogs that they are selling to help to pay for this, because if their employees aren't truly being screened every day, we are asking for a problem.

And, certainly, Ms. Lowey and I work together on this bill. It is something that needs to be done, but five airports, it is a good start

and certainly your announcement yesterday, which was very timely in light of this hearing today, we need to have a better system there at the airport.

Let me ask you a question: If a person is working for a vendor at the airport and they are screened, does it also include checking for the fact that perhaps they are an illegal immigrant?

Mr. HAWLEY. Yes.

Ms. BROWN-WAITE. And illegal immigrant employees do not pass the test; is that correct?

Mr. HAWLEY. That is supposed to be the program. There have been some cases where with false, in the past, social security numbers, things like that. So there is a criminal history records check and a watch list check. And to that, the program that we have added here in the past number of months includes the immigration check.

Ms. BROWN-WAITE. Sir, when you talk about random screening, Orlando already had random screening, and yet this incident occurred. Do you think that passengers should have random screening, and do you think TSA workers should have random screening?

Mr. HAWLEY. Well, they all do, and I think everybody should. And perhaps you were not here earlier when I addressed the Orlando issue. I don't want to get into the specific details of a live case, but that, as history will show, did not involve a risk of terrorism on that particular flight. It did, however, present some interesting learnings about operations of people who are breaking the law in an airport environment, which obviously we have paid a lot of attention to.

Ms. BROWN-WAITE. Sir, I want to work with the agency to accomplish the goal of making sure that passengers are safe. If the TSA workers have to go through that line, every member of Congress has to go through that line, every little old lady in a wheelchair has to go through that line, then it just is unfathomable why we are not taking that extra step. Because, obviously, as proven in the Orlando case, random doesn't work.

Mr. HAWLEY. Well, it is a very different environment. In the sterile area that you get screened to go in as a passenger is a very limited holding tank that is swept for objects and is kept sterile. The airport work environment where workers work is a city, and it is not practical to have that be a sterile environment.

What you want to do is keep track of the people inside. Know who is there, know where they are and what they are doing, because everything you need to do a terrorist act is already on the inside, and to check just what they are bringing in from the outside is not sufficient security.

Ms. BROWN-WAITE. I have one more question, Madam Chair, if you will indulge me.

In light of the fact that you have found illegal aliens who have the employee cards, are you regularly following up at doing at that point at least some random checking to see if we have illegals working at the airports?

Mr. HAWLEY. Yes, we do. As part of the program I mentioned back in the back of the airport on these ADASP programs, we check not only what they have on them, who they are, valid credentials, all of those things are checked, including vehicles, vehicle

searches. There is nothing on the airport that is exempt from TSOs out there screening at any time.

Ms. BROWN-WAITE. Thank you, Madam Chairman.

I yield back the time.

Ms. JACKSON LEE. We yielded the gentlelady, with unanimous consent, an additional 1 minute.

I thank the distinguished gentlelady for her questions, and I now yield to Mr. Perlmutter, the distinguished gentleman from Colorado, for 5 minutes.

Mr. PERLMUTTER. Thank you, Madam Chair.

Mr. Hawley, it is nice to meet you in person.

And, first, I would like to thank you and TSA for responding to some questions I had concerning an examination by the Red Team conducted at the Denver International Airport. I do want to say that you were very responsive, as were people within your organization, in getting back to me. So thank you.

Mr. HAWLEY. Yes, sir.

Mr. PERLMUTTER. But I do want to dig a little deeper into that whole kind of approach. And now I have had an opportunity to meet with Red Team members, to talk to you about this a little bit, to go out to the Denver International Airport. And the issue was that the airport did not do well on an examination, in effect, by a team of your investigators, your experts who kind of probed for holes in the system.

After having met with everyone, it seemed to me that the electronics did a pretty good job. It was more of a personnel kind of an issue. And in Colorado, if I am not mistaken, we have gone from about 1,100 screeners 3 or 4 years ago, we are now down into the neighborhood of about 700 screeners, and we have many, many, many more passengers going through that airport. And I am just wondering if we are taxing our personnel in a way that doesn't enhance our security.

And if you could comment on that, I would appreciate it.

Mr. HAWLEY. Sure. Thank you, and I think you are raising a very important issue.

As you know, IED detection is our number one priority at the passenger checkpoint, and it is, by far, the thing we spend the most time on. And the Red Team testing you mentioned is directed at the people, because we already know what the machines can do. We have taken the labs; we know exactly what they can do. So what we need to test and probe is what is the human factor, how do we better train, how do we better test?

So we send inspectors out there who know the entire system, know the vulnerabilities, and they probe those vulnerabilities to understand what are the human factors we can add that would cover for machine vulnerabilities. And that is an ongoing process, as you know.

As to the number of people, it is always a tough management job to get the right number of people, and we have been able with—and, frankly, I have to give credit to our officers for improving their own effectiveness and efficiency in cutting down absences, working with us to reduce injuries, and some of the human resource things have enabled us to generate screening capacity by fewer people leaving and more training, things like that.

So we look at flight by flight what the TSO requirement is. We did build in the ADASP program, I mentioned earlier, and I think, as we noted last summer, Denver was supposed to be a big disaster in Memorial Day and over the holidays, Labor Day and Thanksgiving, frankly. And we stepped up, and when we had the snow in December, as you know, we flew in people from around the country to keep Denver fluid.

So my commitment to you and the people of Denver and the city of Denver is to keep the airport fluid, effective and not have security be a barrier toward the purpose of the airport.

Mr. PERLMUTTER. And I appreciate that, and, I guess, I think, the tension, and you have described the tension, the tension is between moving people through, getting them on their plane, but also making sure that we have proper security.

And I understand this tension. And I guess what I am saying is your organization—there is a point in any organization, business or otherwise, where you can hit efficiency and then you cut to the bone, and when you cut to the bone, you screw up the mission. And my warning to you is that you are at the bone, and you may not think so, but just my rump opinion, my observation is you are close, if you are not there.

The other thing I would say, and I have some concern, is you try to meet the rush hours, the morning rush hour, the evening rush hour and then it ends up in, kind of, the split shifts or you are looking at hiring part-time folks. And with this particular security issue, I am concerned about that, whether or not you are going to get the kind of people who will be devoted to the agency, be long-term employees who will do a good job. That is just my word of advice.

And, Madam Chair, I will yield back.

Thank you.

Ms. JACKSON LEE. We thank the distinguished gentleman.

And I am now pleased to yield 5 minutes to the distinguished gentlelady from New York, Ms. Clarke, who has a few large airports in her area, New York City, Brooklyn.

Ms. CLARKE. Thank you so very much, Madam Chair.

After the attacks on New York and Washington, D.C., on 9/11, the American people had the expectation that the government would ensure that such a situation could never happen again. Congress reacted by passing a variety of reforms aimed at preventing airline passengers from carrying anything on board a plane that can threaten lives. However, recent events that have occurred at airports all over America have convinced me that not nearly enough is being done to prevent harm coming from airport workers.

While the vast majority of airport and airline employees are honest, hardworking people, there are inevitably a few individuals that can and may view working at an airport as a way of getting around screening. This is a major vulnerability, and I think we have all acknowledged that.

I live in Brooklyn and represent a large district in Brooklyn, which is under the busiest air corridor in the country. There are three very large airports within just a few miles of my district, and there is no reason why we should not do everything possible to protect those who fly and those on the ground.

If 100 percent screening of airport workers can be accomplished, I see no reason why we should not do this.

Secretary Hawley, it is good to see you once again, and I know that these are really complex issues that you are having to deal with here, but if Heathrow and Miami International Airport and other airports have successfully implemented 100 percent worker screening with success, why wouldn't it work systemwide?

Mr. HAWLEY. I think the type of screening for passengers is of a different nature given the purpose of passenger screening is to make sure that objects that can be used to have a terrorist attack don't get onto a plane; whereas, it is a very different thing in the secure area of a working factory, basically, where you have all the chemicals that you could imagine, tools, lots of things, not to mention the aircraft itself.

So I believe from a security perspective, it is more important to really be sure of who these people are, have the training—and I know we have talked of this in the mass transit environment, but it is exactly the same issue of increase the training and the ability to, as you said to me, once you see something and say something, who do you tell it to and what do you do, but to have that worked into the airport environment as well.

And I think that is an immediate, effective security measure that is worth more to us in the flying public than trying to figure out which screwdriver—figuring out what every duty is for everybody working there. I think there is always a component of checking physically when they come in, and we are happy to work with the committee on pilots to achieve that.

Ms. CLARKE. Yes, because you mentioned in your testimony here today about the sterile environment versus the non-sterile environment. I think the emphasis coming from this subcommittee is that we focus in on that non-sterile environment and create as many opportunities in that environment to deal with the whole issue of who is there, why they are there and what constructs can come from it.

And I don't know whether there has been an analysis or an assessment or even a pilot that begins to get at these answers, but I would suggest to you that it is going to be important from so many different perspectives.

I mean, we don't know under what circumstances someone becomes psychotic, we don't know what drives people to do the things that they do. We look at international terrorism oftentimes as the major threat, but we are finding more and more, as we found, unfortunately, this week, that you may have a troubled individual that shows up to work, recognizes they have the capability to do something demonstrative in terms of destruction, and we are unable to catch it, because we haven't created an environment that would disrupt something like that.

You discuss the possibility of using a biometric card. Other DHS programs, such as US–VISIT has attempted to make use of biometric data on a large scale but have found it highly complicated and difficult, which has often led to failure.

How difficult do you feel it would be to implement such a program for airport workers compared with using existing technology to screen them, and how long do you feel it would take to imple-

ment this in comparison with how long it would take to implement screening technologies similar to what is used on passengers?

Mr. HAWLEY. On the issue of observing someone with erratic behavior, at the checkpoint, if we have got magnetometers, that is not going to pick it up. But the behavior observation and the training, that is one thing we have learned this week, is that there are signs if you are looking for them and prepared to act. So we are in full subscription with integrating the behavior observation to pick up both the foreign terrorist as well as anybody who would do otherwise harm.

And on the biometric, as everybody knows, that is a very complicated technology, and we are breaking new ground at DHS with these programs, and the transportation worker identity credential, which we are doing in the maritime environment, is breaking new ground that we can use the data from that to use in the airport environment. And that is what gives me the optimism to think that we can move forward.

And there have been some standards of interoperability done in the airport community, already established, like in Registered Traveler. So we are in the ballpark. I think that is the one that is the furthest out of the measures that we are talking about, and what in my calendar is to figure out in the 4-to 6-month period what the parameters are and the specs and this is what it is and then figure what that costs.

And it is critical—I think you raised an excellent point—it is critical we not go to gold-plated, that we go to something that is effective, gets the job done and can be quickly deployable.

Ms. CLARKE. Thank you very much, Secretary.

Thank you, Madam Chair.

Ms. JACKSON LEE. Let me thank you, Mr. Hawley, for your attention to these matters. Certainly, I think together we have a collective commitment to ensuring the safety of all of our airports. I have mentioned, though, the jurisdiction in this committee may go even beyond TSA, even questions about general aviation we must address.

I leave you simply, as I bring forward the second panel, one, I think you will find a theme in this larger committee and the subcommittee a great concern for our employees, both in terms of training, in terms of security, whether it be those who work in the airports or whether it be our pilots and flight attendants. We will be looking forthwith on added training measures for both pilots and flight attendants. And so we are equally attendant to our, if you will, core of workers. We thank them for their service, but we know there have been breaches.

And so I think the concern is, as I ask for a sense of urgency from the agency as we look at legislation this coming week, be reminded that during the breaches our airport employees cut across very serious products, be they weapons, be they chemicals or other manner that could be used to create havoc. It is in the breach, it is in the lapse that comes tragedy and disaster. We don't have those excuses.

So I thank you and would look forward to working with TSA to ensure that we have a sense of urgency in this committee and a sense of urgency to be able to create the right mix of legislation

and policy that is moved as quickly as possible in order for us to leap across the breach and to close the breach. I think that is an enormously important challenge that we have.

Thank you for your testimony.

The members of the subcommittee may have additional questions for Administrator Hawley. We will ask you to respond to those questions expeditiously, Administrator, in writing, and at this time, the committee shall move to the next panel.

Call that a little bit of musical chairs. You did that very well.

[Laughter.]

At this time, I would like to welcome the second panel of witnesses.

Our first witness will be Ms. Lauren Stover, assistant aviation director, Security and Communications for Miami-Dade Aviation Department. In this capacity, Ms. Stover handles all communications responsibilities for the department and assumed a key role in the management of airport security.

A 23-year veteran of Miami-Dade County government, she returned to the Miami-Dade Aviation Department after a stint in a leadership role within the U.S. Department of Homeland Security.

Our second witness is Greg Principato, president of Airports Council International—we thank you for being here—North America. Mr. Principato oversees the leading association of airports and airport-related businesses in North America, which enplane nearly all of domestic and international airline passenger and cargo traffic on the continent. And I am always reminded by my director, Rick Vacar of the importance of ACI. I think I have been attending with him for a number of years.

So we welcome you again.

The final witness of this panel is Mr. William E. Holden, senior vice president of operations, Covenant Homeland Security Solutions. Before joining CHSS, Mr. Holden spent 30 years in civil aviation, holding management positions of various levels in Pittsburgh, Philadelphia, Newark, Miami, Boston, LaGuardia and Washington National Airports. He also held director-level positions in passenger services with Pan American and Northwest Airlines.

Let me indicate to the witnesses that we will proceed with this hearing. You may see the distinguished gentlelady from New York to take the gavel for a moment. We are in several committees at once, votes on the floor; however, I, as the chair, will return and be able to engage with you.

So without objection, the witnesses' full statements will be inserted into the record.

I now ask each witness to summarize his or her statement for 5 minutes, beginning with Ms. Stover from Miami-Dade Aviation Department.

And we welcome you to Washington.

STATEMENT OF LAUREN STOVER, ASSISTANT AVIATION DIRECTOR FOR SECURITY AND COMMUNICATIONS, MIAMI-DADE AVIATION DEPARTMENT

Ms. STOVER. Thank you very much.

Good morning, Madam Chairwoman, Ranking Member Lungren and members of the subcommittee. I thank you for having a hearing on this very important issue of screening airport employees.

As you know, since 1999, we have been performing security screening of all employees working in secure and restricted areas of Miami International Airport. This practice grew out of necessity, resulting from a 2-year undercover drug smuggling operation, not unlike the one that occurred Orlando International Airport.

In response, MIA implemented a comprehensive security enhancement program including, most notably, the screening of all employees with access to secure areas of the airport. We began conducting criminal background and warrants checks for employees working at the airport needing access to these restricted areas. We hired more security staff and, in short, dramatically beefed up our overall security program such that in many ways MIA was ahead of its time in terms of security measures that now, in the post-9/11 era, are completely applicable to neutralizing a potential terrorist threat.

The overall issue we had to address in 1999, and what Congress will be deliberating this year, is how to keep airport employees from using their access to restricted areas as a means to conduct illegal activities. At MIA, we have 30,000 people working at the airport, 27,000 of whom have access to restricted areas.

One hundred percent of the individuals accessing the secure area through the terminal are screened by the magnetometer, and their personal items are subject to X-ray inspection. Employees are also required to log in and log out throughout our access control system when beginning and ending their shifts.

We contract with a private security firm to operate our four employee-only screening checkpoints for personnel that work in the aircraft ramp area. In the terminal area, working closely with our air carriers and employee unions, we incrementally reduced the 34 unmanned employee entrance areas to the four that we have today.

We have implemented security directives that specify the types of items employees can carry with them into SITA areas. For instance, many employees carry tools that are necessary for work but otherwise would not be allowed through a standard passenger checkpoint. Employees who work in the sterile areas within the terminal that are beyond the passenger security screening checkpoint are screened by TSA.

With background checks and comprehensive security measures, including behavior pattern recognition, which I will discuss later, we have a layered approach to security, and we ultimately know who these people are and what they are doing.

We spend about $2.5 million each year on the security guard services to implement this employee screening program. As I said before, our security program is a multilayered approach and we work closely with our local law enforcement and with our federal partners in the Department of Homeland Security, as well as the U.S. Department of Justice, such as what we are doing currently right now in Miami, as I speak to you today.

We regularly need and exchange information. Also conducts sweeps with these law enforcement partners to ensure that employees are not engaged in criminal activity.

In addition to conducting comprehensive background checks, interagency sweeps and screening employees with access to secure areas, another security layer that we have at MIA that I am extremely proud of because we are a leader in this area, is an airport-wide behavioral analysis program.

The behavior pattern recognition, or BPR, as it is termed, is a security technique originated by Rafi Ron, who is the former security director for Ben Gurion, an airport in Tel Aviv, whereby people are trained to detect suspicious individuals based on behavior rather than ethnic background. To date, more than 1,500 employees at MIA have received the training, and sessions will continue with the goal of training all 30,000 employees.

As you look at ways to improve security at our nation's airports, specifically through employee screening, I would like to say that all airports are truly different with respect to their configuration, their security programs and the threat analysis. A one-size-fits-all solution is not appropriate.

A federal approach to employee screening must take into consideration that most airports are financially unable to dramatically increase expenditures any more than what they have done since 9/11. In fact, most airports already are dealing with paying for unfunded federal mandates, such as the inline explosive detection system that we are currently installing at MIA. Airport facilities differ and the way employees get to their jobs differ, but there is common ground. And with input from airports, we can assist in crafting airport employee screening legislation to better secure our nation's airports and passengers.

I would like to leave you with some thoughts from our perspective on employee screening. First, any national program that mandates employee screening must be properly resourced and funded. Second, different standards must be established. The protocols and standards that are appropriate screening are different than those appropriate for passenger screening.

Third, we believe the emphasis should be on stopping ill-intended individuals. And, finally, a layered approach to security is our best bet from those who would do us harm.

I thank you for the privilege of sharing our experiences and thoughts, and I look forward to answering your questions. And thank you for having me here today.

[The statement of Ms. Stover follows:]

PREPARED STATEMENT OF LAUREN STOVER

Good morning Madame Chairman, Ranking Member Lungren and Members of the Subcommittee. I thank you for having a hearing on this very important issue of screening airport employees. As you know, since 1999, we have been performing security screening of all employees working in secure and restricted areas of Miami International Airport. This practice grew out of necessity as we discovered an organized narcotics smuggling operation not unlike the recent incident that occurred at Orlando International Airport.

In response to the drug smuggling activities that involved airline employees, a comprehensive security enhancement program, including most notably the screening of all employees with access to secure areas of the airport, was implemented at MIA.

We began conducting criminal background and warrants checks for employees working at the airport needing access to secure and restricted areas. We hired more security staff and, in short, dramatically beefed up our overall security program such that in many ways, MIA was ahead of its time in terms of security measures

that now, in the post 9–11 era, are completely applicable to neutralizing a potential terrorist threat.

The overall issue we had to address in 1999, and what Congress will be deliberating this year, is how to keep airport employees from using their access to restricted areas as a means to conduct illegal activities. First, let me say as an airport employee for many years, most of us are good, hardworking people, but a few, with ill intentions, can do a lot of damage. In conducting employee screening, we are reducing the "insider threat" which is a critical element of our security program.

Let me briefly describe who these airport employees are. There are airport employees such as myself that work for the operator of the airport, which in most cases is the local government or an airport authority. The vast majority of people who work at the airport, however, work for airlines, vendors and tenants, many of whom have access to restricted areas in order to perform their duties.

At MIA, we have 30,000 people working at the airport. My security department manages the credentialing of these employees with identification media/or ID badges. In the secure areas of the airport, including the SIDA area—or Security Identification Display Area—employees must always have on visible display the ID media issued by my security division at the airport. All airport employees are trained to challenge anyone not displaying a proper ID in the SIDA.

Criminal History Background Checks are conducted on all employees who have a need to access secure areas. We color-code our ID badges which helps anyone be able to immediately identify the specific area where an employee will work, such as on the airfield or inside the terminal beyond the security checkpoint, etc. At MIA, 100% of the individuals accessing the secure area through the terminal are screened by magnetometer (or walk through metal detector) and their personal items are subjected to x-ray inspection. Employees are also required to log-in and log-out through our access control system when beginning and ending their shifts.

We contract with a private security firm to operate our four employee-only screening checkpoints for personnel that work in the ramp area where the aircraft are positioned at gates connected to the terminal. These are the baggage handlers, maintenance personnel and other employees that work directly on airplanes and around the airfield. In the terminal area, working closely with our air carrier and employee unions, we incrementally reduced the 34 unmanned employee entrance areas to the four we have today. We have implemented security directives that specify the types of items employees can carry with them into SIDA areas. For instance, many employees carry tools that are necessary for work but otherwise would not be allowed through a standard passenger checkpoint. Employees who work in the secure areas *within the terminal* that are beyond the passenger security checkpoint are screened at the passenger security checkpoint by TSA.

With background checks and comprehensive security measures including Behavioral Pattern Recognition which I will discuss later, we have a layered approach to security and we ultimately know who these people are and what they are doing.

We spend about $2.5 million dollars each year to implement this employee screening program at MIA. As I said before, our security program is multi-layered, and we work closely with our local law enforcement—the Miami-Dade Police Department—as well as with our federal partners in DHS—TSA, Immigration and Customs Enforcement, and Customs and Border Protection as well as the U.S. Department of Justice, the FBI and the Joint Terrorist Task Force. We make a point to regularly meet and exchange information in order to allow investigations to proceed without interference and to continue to monitor activity in securing the airport. We also regularly conduct sweeps with these law enforcement partners and our canine teams to ensure employees are not engaged in criminal activity.

In addition to conducting comprehensive background checks, inter-agency sweeps and screening employees with access to secure areas, another security layer that we have at MIA that I am extremely proud of because we are a leader in this area is an airport-wide behavioral analysis program. Behavior Pattern Recognition, or BPR, is a security technique originated by Rafi Ron, the former security director for Ben Gurion Airport in Tel Aviv, where people are trained to detect suspicious individuals based on behavior rather than ethnicity.

To date, more than 1,500 employees at MIA have received the training, and training sessions will continue over the next two years with the goal of training all 30,000 employees at MIA. BPR will be permanently embedded into the fiber of the airport's security program, and BPR training will be required for employees renewing their airport ID badges. In March 2007, MIA was the first airport to host a national BPR training session for airport law enforcement officers.

As you look at ways to improve security at our Nation's airports, specifically through employee screening, I would like to say that all airports are truly different with respect to their configuration, security and threat analysis. A one-size fits all

solution is not appropriate. A federal approach to employee screening must take into consideration that most airports are financially unable to dramatically increase security expenditures any more than what they have done since 9/11. In fact, most airports already are dealing with paying for unfunded federal mandates such as the in-line Explosives Detection System we are installing at MIA. Given our financial constraints, we have been forced to defer other capital projects in order to fund our North Terminal EDS project. To date, TSA has not committed funding.

Airport facilities differ and the way employees get to their jobs differ, but there is common ground and with input from airports, we can assist in crafting an airport employee screening legislation to better secure our Nation's airports and passengers.

I would like to leave you with some thoughts from our perspective on employee screening. First, any national program that mandates employee screening must be properly resourced and funded. Second, different standards must be established. The protocols and standards that are appropriate for employee screening are different than those that are appropriate for passenger screening. Third, we believe the *emphasis* should be on stopping ill-intended individuals from accessing the secure area. And, finally, a layered approach to security is our best defense from those who would do us harm.

I thank you for the privilege of sharing our experiences and thoughts and look forward to answering your questions.

Ms. JACKSON LEE. Thank you very much for your testimony.

I now would like to recognize Mr. Holden with Covenant—I have moved ahead. I would like to recognize Mr. Principato, with ACI, to summarize his statement for 5 minutes.

Thank you.

STATEMENT OF GREG PRINCIPATO, PRESIDENT, AIRPORTS COUNCIL INTERNATIONAL-NORTH AMERICA

Mr. PRINCIPATO. Thank you, Chairwoman Jackson Lee, Ranking Member Lungren and members of the subcommittee. Thank you for the invitation to appear today. I am here to offer the views of America's airport security and on improvements to enhance the systems currently in place.

As president of Airport Council International-North America, I am testifying today on behalf of the local, regional and state authorities that own and operate commercial service airports. As has already been stated by the chairwoman, our member airports enplane nearly all of the domestic and international and passenger cargo traffic in North America.

Nearly 400 aviation-related businesses are also members of ACI-North America.

Madam Chairwoman, we commend you for holding this hearing today. Each day, airports work to ensure that our facilities are safe and secure for our passengers and for our employees. To this end, airports partner with airlines, tenants, TSA and federal and state and local law enforcement to maintain and develop a comprehensive layered security system that can quickly respond to new and evolving threats.

A critical part of this wide-ranging structure is ensuring that individuals with access to secure areas are sprained as part of the risk-based security regime that makes the best use of TSA and airport resources.

Before additional security measures are mandated, it is important to understand the multilayered system currently in place for individuals with access to secured areas at airports. Airport, airline or other tenant employees seeking unescorted access privileges in the secured area of airports undergo a finger-print based FBI

criminal history record check. These individual are continually checked against federal terrorist watch lists.

In addition, TSA conducts a security threat assessment to verify the individual's identity, employment eligibility and citizenship status.

Access control systems are also an important part in ensuring airport security. These systems range from key or cipher locks to sophisticated, fully automated systems utilizing biometric data. Most access control systems are also supplemented by closed-circuit television to allow monitoring of the critical areas from a centralized control room, audible alarms to enunciate breaches and patrols by public safety and law enforcement personnel.

Vehicles and equipment seeking access to these areas are inspected by local law enforcement or specially trained public safety personnel. Some new generation access control systems within the secure areas.

Airport, airline and tenant employees undergo security training specifically tailored to the airport. Additionally, the TSA Aviation Direct Access Screening Program, ADASP, subjects employees and their property to random screening as they enter the secured area. Anywhere on the airport, at any time, employees, including airport directors, know they may encounter TSA screening.

Now, as was discussed before by Administrator Hawley, ACI-North America has been working with TSA, with the American Association of Airport Executives and our airport members to develop programs for even more robust employee screening. The program under discussion would not replicate the stationary process currently in place for passengers and their baggage, as the work environment for airport workers has already been discussed, presents far different challenge, security challenges, and requires measures targeted to meet those challenges.

It includes the use of behavior recognition techniques, targeted physical inspections, enhanced employee training to raise awareness of suspicious behavior, development of a certified employee program, expansion of the use of biometric access controls and deployment of additional airport surveillance technology.

TSA, airports, airlines and employee representatives are working to refine the specific procedures that would be incorporated into the pilot program. We believe that work can be completed in about the next 90 days or so. ACI-North America is recommending that the pilot program using these techniques be conducted for at least 180 days to assess the improvement in aviation security, the impact on airport and airline operations and the cost of the program.

Assuming Congress appropriates the necessary funds to implement the plan, further deployment could then occur.

This approach would also incorporate the latest intelligence information to allow more nimble and effective security measures, which could be modified quickly to address new and emerging threats. The pilot would also allow different combinations of programs and technologies to be evaluated to determine which provide the greatest security benefits and which are appropriate for airports of varying sizes and configurations.

I want to again emphasize that airports are committed to working with you and with Congress to enhance the already effective

airport security system with risk-based measures. We believe that a risk-based program, developed collaboratively by airports, airlines and TSA, will enhance the security of the traveling public by strengthening employee screening while appropriately using technologies and resources across the industry.

The members of ACI-North America thank you for inviting me to testify and we look forward to working with you, and I look forward to your questions.

Thank you.

[The statement of Mr. Principato follows:]

PREPARED STATEMENT OF GREG PRINCIPATO

Chairwoman Jackson-Lee, Ranking Member Lungren, and members of the subcommittee, thank you for the invitation to appear before the subcommittee today to offer the views of America's airports on airport security and improvements to enhance the systems currently in place. As the President of Airports Council International—North America (ACI–NA), I am testifying today on behalf of the local, regional, and state governing bodies that own and operate commercial service airports in the United States and Canada. ACI–NA member airports enplane more than 95 percent of the domestic and virtually all the international airline passenger and cargo traffic in North America. Nearly 400 aviation-related businesses are also members of ACI–NA.

Madam Chairwoman, we commend you for holding this important hearing. Each day, airports work to ensure that our facilities are safe and secure for passengers and employees. To this end, airports partner with airlines, tenants, the Transportation Security Administration (TSA), and Federal, State, and local law enforcement to maintain and develop a comprehensive, layered security system that can quickly respond to new and evolving threats. A critical part of this wide-ranging structure is ensuring that individuals with access to secure areas are screened as part of a risk-based security regime that makes the best use of TSA and airport resources.

Before additional security measures are mandated it is important to understand the multi-layered system currently in place for individuals with access to the secured areas at airports. First, persons employed by the airport, airlines or other tenants seeking unescorted access privileges within the controlled areas of airports must provide the airport sponsor with two forms of government-issued photo identification, be authorized to work in the United States of America, and undergo a fingerprint-based FBI criminal history records check to ensure that they have not committed any of an explicit list of crimes designated by Congress during the prior 10 years.

Some airports, with TSA approval, have implemented more rigorous background check standards, verifying information for the past 20 years. Further, at the time of initial employment and throughout the period where access privileges are authorized, these individuals are continually checked against the federal terrorist watch lists developed by TSA, the Department of Homeland Security (DHS) and the intelligence agencies. In addition to the criminal history records verification and terrorist watch list checks, the TSA conducts a security threat assessment (STA) to verify the individual's identity, employment eligibility and citizenship status.

Access control systems are also an important component in ensuring airport security. These systems have been are in place for many years at airports and range from key or cipher locks to sophisticated, fully automated systems utilizing biometric data. The components provide security beginning at the public area through the security identification display area (SIDA). All certificated airports designate these zones in their Airport Security Plans (ASPs) and implement measures to restrict access to those with an operational need to enter the area. Airports must also immediately report to TSA any change in an individual's badge status to ensure that individual's access to the secured areas of airports will be revoked.

Most access control systems are also supplemented by closed circuit television to allow monitoring of the critical areas from a centralized control room, audible alarms to annunciate breaches, and patrols by public safety and law enforcement personnel. Vehicles and equipment seeking access to these areas are inspected by local law enforcement or specially trained public safety personnel. Some new generation access control systems allow for tracking of authorized vehicles within the secure areas.

Airport, airline and tenant employees undergo initial and recurrent security training, specifically tailored to the airport. The training emphasized the individual's re-

sponsibilities and duties while working in the secured area of the airport, including the importance of challenge procedures and quickly contacting airport authorities of unusual activities or possible threats.

Additionally, the TSA Aviation Direct Access Screening Program (ADASP) subjects employees and their property to random screening as they enter the secured area. It is well established that random security checks provide an effective deterrent to both criminal and terrorist activities. Anywhere on the airport at any time, employees know they may encounter TSA screening. We believe that random checks under the ADASP make airport security unpredictable, thus making it difficult for terrorists to ascertain operational patterns that can be exploited.

ACI–NA has been working with TSA, the American Association of Airport Executives and our airport members to develop programs for even more robust employee screening. The program under discussion would not replicate the stationary process currently in place for passengers and their baggage, as the work environment for airport workers has different security issues that must be addressed with measures targeted to meet those potential vulnerabilities. Instead, it includes the use of behavioral recognition techniques and interviews before employees enter the sterile and security areas, targeted physical inspections, enhanced employee training to raise awareness of suspicious behavior, development of a certified employee program, expansion of the use of biometric access controls and deployment of additional airport surveillance technology. ACI-NA recommends that a pilot program using these techniques be conducted for at least 180 days, to assess the improvement in aviation security, the impact on airport and airline operations and the costs of the program. Assuming Congress appropriates the necessary funds to implement the plan, a phased deployment of the program to the 452 commercial U.S. airports could then occur.

Implementation of this six-point program would incorporate the latest intelligence information to allow more nimble and effective security measures, which could be modified quickly to address new and emerging threats. Such a program would also allow different combinations of programs and technologies to be evaluated to determine which provide the greatest security benefits and which are appropriate for airports of varying sizes and configurations.

As you know, Miami International Airport and Orlando International Airport have already implemented a different approach for employee screening. We understand the circumstances which lead to these ACI–NA member airports establishing measures tailored to their unique environment and security challenges. ACI–NA supports the right of airports to exceed federal or state regulatory requirements if they believe the additional security procedures and/or equipment provide a benefit for their passengers and employees.

I want to again emphasize that airports are committed to working with Congress to enhance the already effective airport security system with risk-based measures. We believe that a risk-based program, developed collaboratively by airports, airlines and TSA, will enhance the security of the traveling public by strengthening employee screening while appropriately using resources across the industry.

The members of ACI–NA and I thank you for inviting me to testify today and we look forward to continuing to work with you on this important issue. I'll be pleased to address any questions you might have.

Ms. CLARKE. [Presiding.] Thank you for your testimony.

And I now recognize Mr. Holden, with Covenant Homeland Security Solutions, to summarize his statement for 5 minutes.

STATEMENT OF WILLIAM E. HOLDEN, SENIOR VICE PRESIDENT OF OPERATIONS, COVENANT HOMELAND SECURITY SOLUTIONS

Mr. HOLDEN. Thank you. Ms. Clarke, ranking member of the subcommittee, I would like to thank you each of you for inviting me to participate in a hearing to discuss airport security.

By way of background, Covenant Aviation Security was awarded a contract as part of a Transportation Security Screening Pilot Program on October 10, 2002. We are currently providing both passenger and baggage screening at San Francisco International Airport, a category X airport, and also at Sioux Falls Regional Airport, a category II airport.

Covenant was the only private contractor to be awarded two airports during the pilot screening program.

I would like to point out the compressed timelines under which the award was made on October 10 until staffing the checkpoints on November 19, 2002 and providing full trained screeners for checked baggage on January 1, 2003.

Covenant was successful in meeting both of these federally mandated deadlines. Covenant successfully deployed over 1,100 security screeners to all passenger checkpoints at San Francisco International Airport and Tupelo Regional Airport during the very brief 39-day transition period. Additionally, Covenant staffed all baggage checkpoints by January 1, 2003 for a total of 1,453 screeners hired, trained and deployed within the TSA-mandated timelines.

Covenant was awarded screening operations at Sioux Falls in February 2006. Tupelo Regional Airport was awarded to Trinity Technology in May of 2006 as a small business set aside. Covenant provides management services for Trinity.

The Covenant team offers extensive experience in airport operations, security and personnel management capable of providing the government cost effective and value added solutions.

Currently, at both San Francisco International and the Sioux Falls Regional Airport, Covenant Aviation contract scope has been increased by the TSA to include Aviation Direct Access Screening Program, ADASP.

ADASP screening entails the screening of airport personnel who have access to secure areas of the airport. Airport personnel having the appropriate credentials and access rights can enter into the airport sterile area without going through checkpoint security.

Through the ADASP, airport personnel and their belongings are subject to rigorous screening standards to prevent the introduction of prohibited items into an airport's sterile area. The ADASP represents a significant step forward by the TSA to ensure the safety of the flying public.

ADASP was implemented by TSA in 2007 and requires additional procedures to expand screening to include direct access points into the airport operations area, AOA. It is important to note that there is an extensive background check process for all airport community employees.

ADASP is conducted on a random and unpredictable basis to accomplish the following: Look for improper ID media, ensure that all checked IDs do not show signs of tampering, look for non-visible airport ID media, ensure that prohibited items on the TSA prohibited list do not gain access to the AOA, and, five, check individuals and their accessible property entering direct areas other than checkpoint entries, resolving all alarms.

The majority of all employees that work in the airport community and possess a badge issued by the security access for San Francisco International as well as their belongings go through the same screening process as the traveling public. They proceed through a walk-through metal detector and their personal or job-related possessions are screened by an X-ray machine. If there is an alarm of any kind they are subject to hand wanding, bag searches or a pat down of their possessions. They are subjected to

the screening process every time they leave the sterile area and wish to re-enter.

Employees in the airport community are airline employees, inclusive of management and flight crews, vendors working for the airlines or city employees. In San Francisco and Sioux Falls, the certified screeners that work for Covenant must go through the security check point each time they enter the sterile area.

Covenant strongly supports the screening of all employees in accordance with the Aviation and Transportation Security Act of 2002. I stand for your questions.

[The statement of Mr. Holden follows:]

PREPARED STATEMENT OF WILLIAM E. HOLDEN

Chairwoman Jackson Lee, Ranking Member Lungren, Members of the Subcommittee on Transportation Security and Infrastructure Protection—I would like to thank you for inviting me to participate in today's hearing to discuss Airport Security.

BACKGROUND

Covenant Aviation Security was awarded a contract as part of the Transportation Security Administration's (TSA) Security Screening Pilot Program on October 10, 2002. We are currently providing both passenger and baggage screeners at San Francisco International Airport, a Category X airport, and Sioux Falls Regional Airport, a Category II airport. Covenant was the only private contractor to be awarded more than one airport under the Privatization Pilot Program (PP5). I would like to point out the compressed time frame from contract award on October 10, 2002, until staffing all checkpoints on November 19, 2002, and providing fully trained screeners for checked baggage on January 1, 2003. Covenant Aviation was successful in meeting both of these federally mandated deadlines.

Covenant successfully deployed over 1,100 security screeners to all passenger checkpoints at San Francisco International Airport (SFO) and Tupelo Regional Airport (TUP) during the very brief 39-day transition period (October 10, 2002—November 19, 2002). Additionally, Covenant staffed all baggage checkpoints by January 1, 2003 for a total of 1,453 screeners hired, trained and deployed within the TSA-mandated timelines. Covenant was awarded screening operations at Sioux Falls Regional Airport in February 2006. Tupelo Regional Airport was awarded to Trinity Technology Group in May 2006 as a small business set aside contract with the TSA. Covenant provides management services for Trinity.

The Covenant team offers extensive experience in airport operations, security and personnel management capable of providing the Government cost effective and value added solutions. Our company mission states our commitment to provide dedicated aviation security services for the safe and efficient movement of people and cargo within the United States and its territories. One benefit Covenant has capitalized on is the dedication and support we have received from the Airport Directors, Mr. John Martin of San Francisco, Mr. Terry Anderson of Tupelo and Mr. Mike Marnach of Sioux Falls.

In addition, our collaborative relationships with the Federal Security Directors' in San Francisco, Mr. Ed Gomez and Mr. Mark Heisey in Sioux Falls, South Dakota have enabled us to provide exceptional service and is a contributing factor in successfully maintaining the mission focus. The "Team SFO" and "Team FSD" concept represents the joint efforts of Airport Management, the Federal Security Director including their staffs and Covenant. These relationships were built over time and a result of Covenant consistently demonstrating the ability to overcome challenges and supporting the TSA and its mission.

EMPLOYEE SCREENING

At both San Francisco International and the Sioux Falls Regional Airport, Covenant Aviation Security's contract scope has been increased by the TSA to include Aviation Direct Access Screening Program (ADASP) screening. ADASP screening entails the screening of airport personnel who have access to secure areas of the airport. Airport personnel having the appropriate credentials and access rights can enter into the airport sterile area without going through checkpoint security. Through the ADASP, airport personnel and their belongings are subject to rigorous screening standards to prevent the introduction of prohibited items into an airport's

sterile area. The ADASP represents a significant step forward by the TSA to ensure the safety of the flying public."

ADASP was implemented by TSA in 2007 and requires additional procedures to expand screening to include direct access points into the Air Operations Area (AOA). It is important to note that there is an extensive background check process for all airport community employees.

ADASP is conducted on a random and unpredictable basis to accomplish the following:

i. Look for improper ID media
ii. Ensure that all checked ID's do not show signs of tampering
iii. Look for non-visible airport ID media
iv. Ensure that prohibited items on the TSA prohibited list do not gain access to the AOA
v. Check individuals and their accessible property entering direct access areas other than check point entries, resolving all alarms.

The majority of all employees that work in the airport community and possess a badge issued by the Security Access Office for San Francisco International Airport (SFO) as well as their belongings go through the same screening process as the traveling public. They proceed through a walk through metal detector and their personal or job related possessions are screened by an x-ray machine. If there is an alarm of any kind they are subject to Hand Wanding, bag searches or a pat down of their person. They are subjected to the screening process every time they leave the sterile area and wish to re-enter.

Employees in the airport community are airline employees (inclusive of management and flight crews), vendors working for the airlines or city/airport employees. In SFO and FSD the certified screeners that work for Covenant must go through the security check point each time they enter the sterile area.

CHALLENGES AND IMPLEMENTED SOLUTIONS

Due to the fact the two airports we service are distinctly different (Category X and Category II) they bring individualized operational issues to the table. I will begin by discussing solutions we implemented in San Francisco and Sioux Falls.

STAFFING

The current staffing level in San Francisco is 815 full time employees. The TSA authorized staffing level is 845. Covenant teamed with the FSD, Mr. Gomez and his staff, determined the required hours of operation by incorporating information collected on passenger throughput and passenger waiting time in order to "right-size" the screener workforce. Covenant has been successful in reducing the number of employees without jeopardizing the level of security, customer service levels or experiencing an increase in wait times.

We currently have 84 part-time employees which provides Covenant the flexibility to schedule those individuals where needed in order to meet the demand. To my knowledge, we were the first airport to establish a part-time workforce.

Sioux Falls is staffed with 32 full time employees and 4 part time employees.

SCREENING CONTROL CENTER

The FSD, Airport Director and Covenant recognized the need for a Command and Control center for the entire airport. Due to the dispersed locations of the checkpoints and three separate terminals it became apparent for a communication system that provided a link to the TSA, airport staff and law enforcement officials.

The Screening Control Center (SCC) concept of Command and Control was developed with the TSA SFO Executive Team and the SFO Airport Commission to provide a centralized resource to improve operating efficiencies of the screening workforce. The SCC is located in the Airport Communications Center and includes a Closed Circuit Television system (CCTV). The SCC is manned 24/7 in order to constantly monitor the operation of SFO's 39 checkpoint lanes and the queuing passengers at checkpoints.

A major function of the SCC operators is to move screeners to checkpoint/ baggage workstations during 'off-peak' hours to work in locations where additional screeners are needed. Additionally, the SCC takes calls reporting out-of-service Government Furnished Equipment (GFE) and oversees the dispatch of Siemens, Boeing and InVision technicians decreasing the downtime of essential screening equipment.

Due to the success we had with the Screening Control Center in San Francisco we implemented it at Sioux Falls at no cost to the TSA or the airport.

SAFETY, ON-THE-JOB INJURIES (OJI) & WORKERS COMPENSATION CLAIMS

Covenant, along with most airports, was experiencing a high number of Worker's Compensation Claims that resulted in significant amounts of money being paid out in claims. Covenant has taken steps to aggressively manage this issue. In early 2003, Covenant management initiated both a part-time screener job classification and a return-to-work program for screeners who have been injured while performing their screener duties. Although they cannot return to full-time employment, they are available to work in a restricted duty capacity (jobs assigned by medical restrictions). Covenant, with FSD approval, has hired a Workers Compensation Specialist to review claims for cost containment and who manages the return-to-work program.

ATTENDANCE CONTROL CENTER (ACC)

Covenant's absentee rates were fluctuating on a monthly basis and at one point went at high as 14.7%. The Covenant management team along with the guidance of the FSD, Mr. Gomez, knew we needed to get this issue under control. In May 2003, Covenant opened the Attendance Control Center and our absentee rate began to decrease almost immediately. Our absentee rate is 3.6%.

The ACC is an innovation that provides a center of communication on current staffing levels at all checkpoints. The ACC works in conjunction with the SCC by reporting actual numbers of personnel at the start of each shift and compares them to the established schedule. The SCC in turn can efficiently reassign personnel to ensure that screening operations are maintained by staffing the areas most critical to operational continuity.

Of particular note, Absent-Without-Leave (AWOL) has been significantly reduced due to management actions taken by Covenant in administering the Attendance and Disciplinary policies. The ACC assists in reviewing and addressing employee attendance performance through counseling or disciplining as appropriate. Having one central location performing this function ensures that applications of discipline for attendance infractions are consistent across all terminal checkpoint and baggage operations.

ASSESSMENT

Covenant recognized the staffing deficiency occurring nationwide. In addition, Covenant could foresee the problems that would occur while waiting, possibly six months, for TSA's subcontractor, CPS to arrive and perform the assessments. During those six months, service levels would be compromised along with rising costs if the usage of overtime hours increased.

With the assistance of the FSD, Covenant has developed a proven approach that was first demonstrated with the hiring of Baggage Handlers. Since then Covenant has conducted several assessments for the recruitment of part-time and full-time passenger and baggage screeners for San Francisco International Airport. The method is a phased approach including three phases (1) recruitment, (2) pre-screening and (3) assessment. Covenant is responsible for the entire assessment process. The percentage of candidates who will successfully meet the full assessment criteria is increased by validating minimum qualification criteria early in the selection process. Pre-screening candidates provides cost-efficient methodologies for ensuring expenses are not incurred for assessing unqualified candidates. Covenant uses actual screeners to assist in panel interviews with candidates so that operational experience is brought to bear in assessing potential employees.

TRAINING

The airport screening environment presents multiple challenges to any training program due in large part to its 24/7 operation and large number of screeners who work various shifts, days of the week, and terminals, yet still must receive the same consistent information and direction that greatly impact security and passenger safety.

Covenant developed a Training Academy that includes an onsite computer learning lab that serves as the "hub" of all training and certification activities. The lab consists of 55 stand-alone PC computers equipped with CD-ROM and headset. Initially, the computers were used primarily for image recognition training—three hours per week. Now screeners have a library of CD-ROMs to choose from that include hidden weapons, screening of footwear, hand-wanding, full body pat down review, back injury prevention, harassment-free workplace, and Hazmat guidelines. In addition, operational equipment can be dispatched to the lab for hands-on training related to operational testing and weekly/monthly maintenance procedures. The Computer Learning Lab has become an integral part of the screener's daily activities—right along side the screening of passengers and checked baggage.

HUMAN RESOURCES

Covenant recognizes the problems federally run airports are experiencing in terms of human resource functions. At times these processes are very confusing and time consuming due to the excessive layers involved in the TSA process.

Covenant realizes the importance of communicating information regarding benefits, policies, and resources available to our employees to maintain positive employee morale. By having a local human resource department Covenant is able to service the employees better. For example, Covenant has the flexibility to promote individuals based on performance and on the other hand can remove an individual from a position if required. Covenant can handle simple matters such as a pay discrepancy the same day. The flexibility has allowed us to implement such employee programs as an Employee Assistance Center, Employee Relations Management system, recognition programs and alternative work schedules without waiting for approval from TSA headquarters.

Having Covenant provide human resource functions allow the FSD to focus on his main objective—security, rather than trying to resolve personnel issues.

BEST PRACTICES (SFO)

Covenant Aviation Security (CAS) is contracted to perform the Aviation Transportation Security Act screening procedures. While fulfilling all of the requirements of the contract and the TSA Standard Operating Procedures (SOP) we have developed some "best practices" that have elevated SFO's performance.

- CAS runs a test every 30 minutes at every operational screening lane of randomly chosen prohibited items (IED's-Improvised Explosive Devices)
- CAS exceeds the hours required for all computer based training, OLC (on-line computer) and TRX (image). CAS has installed computers close to check points and in break areas so employees can readily access all computer based programs.
- CAS has supplied each check point with "image books". The image books are x-ray pictures of actual bags with every day items and some IED and prohibited item materials. The front of the page is the images generated, the back of the page clearly defines the images.
- CAS contracts with companies that covertly try to breach security by having prohibited items or IED parts in their bags or on their person. What separates our testing is CAS makes the testing difficult. The better the score means that we need to make the tests harder. CAS provides a monetary incentive when employees "catch" prohibited items or IED related materials.
- CAS has a pro-active Dual Function Screener (DFS) program. DFS' advantages are improved morale (employees are scheduled for two weeks in baggage and two weeks at check points), heightened skills (because they must know and test in both areas) and operational improvements. If there is an operational problem the DFS program gives CAS flexibility at reacting to security issues.

Best practices that are applicable will be implemented in Sioux Falls.

CONCLUSION

The FSD oversight and partnership we've developed has played a major role in the successful operation at both San Francisco and Sioux Falls airports. The FSDs, Mr. Gomez and Mr. Mark Heisey and their staffs require Covenant to justify/explain the following metrics on a weekly basis: overtime, attendance, OJI's, attrition and wait times for passengers. Recent statistics show that SFO metrics surpass other Category X airports in the Western Area in the areas of attendance, overtime and attrition. The guiding principle for Covenant management is "If we cannot measure it, we cannot manage it."

Covenant strongly supports the screening of all employees in accordance with the Aviation and Transportation Security Act of 2002, Section 44903 of title 49, United States Code.

Ms. CLARKE. I thank all the witnesses for their testimony.

I will remind each member that she or he will have 5 minutes to question the second panel.

I now recognize myself for questions.

My question is directed to Ms. Stover.

Have you had the opportunity to demonstrate your operations and screening techniques for officials at other airports? I got from your testimony that you really want to practice specifically for that airport environment; it is not a one-size-fits-all. But there are certainly some best practices that you have established that can be

adapted to each airport environment that exists, particularly in the areas—that are similar.

Has there been any interest from other airports?

Ms. STOVER. Yes, Ms. Clarke. We have had Orlando Airport come visit us recently, we have had TSA come down and see our operations, and we have had Metropolitan Washington Airports Authority come.

I have offered to the industry, and I do that through this forum today, that any airports that are interested in viewing our operations we would certainly be happy to host them.

Again, we do feel that there needs to be a layered approach to this, working with access controls. We have the ability to be able to restrict the access through the encoding of our ID badges. Recently, I have instituted a call for data on how many doors are being used and those that are not being used, I am shutting down and locking down. My fire access doors I am restricting to those who need access.

So there is a layered approach that we could take to doing this so that there is not just one impenetrable ring but rings of security that would help us to deter any potential acts.

Ms. CLARKE. You also spoke to the cost.

Ms. STOVER. Yes.

Ms. CLARKE. and I would like for you to elaborate a little bit more on that and also state whether you think that there is something that government can do to support.

Ms. STOVER. Certainly. Thank you for the opportunity. Right now, currently, we are—and I don't have the numbers in front of me—but we have $2.5 million that we are expending on the guards. They cost about $23 an hour, we have four checkpoints, we operate 24/7. So we are spending about $2.5 million, including the maintenance costs of the equipment. We also are incurring $300,000 for the recently federal mandated requirement of vendor inspections to the sterile areas. One hundred percent of that is costing Miami Airport $300,000.

We are about to open over 1 million square feet of new terminal in Miami, a whole new south terminal, and in order for me to maintain the current employee screening program that I have, I will need to open another three checkpoints at that cost of $1.3 million, and I am going to look to TSA to provide us with additional walk-through metal detectors for that new terminals, because we are closing down a portion of Miami Airport to develop the whole north terminal. So we are shutting it down, I will have screening equipment there, and I want to move it into the south terminal.

And we have the vehicle access gates where employees enter through the airfield, and we are expending about $1 million there. So we are expending well over $5 million to $6 million on trying to raise the level of security.

Ms. CLARKE. And how are you paying for it?

Ms. STOVER. That is a very good question.

[Laughter.]

That is why we have a leaky roof in Miami Airport. We are just trying to look for grants and ways that we can make it happen. And we are thoughtful and mindful of our airports around the nation that also are in the same financial predicament. We want to

work with the category I, II, III, IVs and Xs and with ACI and AAAE to come up with a practical solution.

We do have an operation going on in Miami Airport right now. Today you may be hearing about it in the press. As a matter of fact, at 2 o'clock where I should have been at a press conference, I am up here with you all.

But we had an investigation that is resulting in some arrests of airport workers. These workers are not physically screened by us. They have access to our cargo areas, so Mr. DeFazio would have been probably interested in that. But we are working with immigration and Customs Enforcement and the U.S. Department of Justice, and we dismantled an operation today in our cargo area.

Ms. CLARKE. I want to thank you for your response and your candor here today.

The chair will now recognize other members for questions they may wish to ask the witnesses. In accordance with our committee rules and practice, I will recognize members who were present at the start of the hearing based on seniority on the subcommittee, alternating between the majority and the minority. And those members coming in later will be recognized in the order of their arrival.

The chair recognizes for 5 minutes the gentleman from Colorado, Mr. Perlmutter.

Mr. PERLMUTTER. Thank you, Madam Chair.

Since we were talking about money just a second ago, I would like to ask the panel, any of you, do you think—have you seen—and I know, Ms. Stover, you are focused on Miami, but all of you, whether or not the TSA is overstaffed?

Ms. STOVER. You want to take that?

Mr. PRINCIPATO. No, I don't think TSA is overstaffed. I heard the points you made earlier, Congressman, and, certainly, several of our members had they been here would be able to tell you that they feel like they need additional resources at the airports to take care of the ever-increasing traffic they are seeing and so forth. So, no, I don't think TSA is overstaffed.

Mr. PERLMUTTER. Mr. Holden, what do you think?

Mr. HOLDEN. Well, when we start our contract in San Francisco, we are over 1,100 screeners. The number today is down to 847, and that includes baggage screening for both passenger screening and baggage screening in January we were over 1,400 employees.

So to answer your question directly, sir, no, I do not feel that they are overstaffed.

Mr. PERLMUTTER. So your experience is similar to what has happened over at Denver's airport. Sounds almost similar numbers, except Denver may be a little bigger cut than you have suffered.

Ms. Stover, what do you think?

Ms. STOVER. Did you want to answer the Denver question?

I can speak to you on behalf of all of the airports. I participate regularly on the conference calls that they have with TSA, with AAAE, with ACI. And, really and truly, the screening allocations across the board, I don't know what the model is but I don't think it is thoughtful in truth into the operations of the airports. We are grossly understaffed, and I can just share that with you.

I used to work for TSA, so I have been on the other side of the fence, and they have done a wonderful job of trying to allocate the cap, but that cap needs to raise.

Mr. PRINCIPATO. If I can just add one point. As Lauren said, TSA is working hard to deal with the cap and so forth and the resources. One of the arguments that we have made is that need over time to move from a labor-intensive to a technology-intensive security system.

Lauren talked before about inline baggage systems, for example. That would be one way to do that; there are many others. Moving from labor-intensive to technology-intensive I think would go a long way toward making the best use of those resources.

Mr. PERLMUTTER. Thank you.

In Denver, we have a lot of inline baggage systems to screen the bags, and I was very interested in looking at that, but there still is the people portion of all this, and my fear is that we are trying to move people along for purposes of getting them on their planes, but then there is so much pressure to move people along, you can make mistakes, and that is my fear.

Here is my political statement—I am glad you answered my question the way I thought you would—is in the emergency supplemental bill that is in conference and will be presented to the president, there is at least $1.5 billion for technology and staff for the staff and for airport security. In the media, there has been a lot of talk about some of the farm pieces or this or that, calling it all pork, but, obviously, in my opinion, spending money on transportation security at our airports or our ports or our borders is not pork.

And I would encourage all three of you to encourage your members or your friends to tell the president not to veto that bill. Thank you.

That is my last question, Madam Chair, and I will yield back.

Ms. JACKSON LEE. [Presiding.] Let me thank Congresswoman Clarke for her dutiful duty.

Mr. PERLMUTTER. Outstanding job.

Ms. JACKSON LEE. And her colleague even adds to that outstanding, and let me also thank Mr. DeFazio in his absence for helping us play a little tag here this morning.

Let me provide a little backdrop to my questioning, and I thank all of you for being here and just to remind us that in the nation's airports, employees and contractors are currently free to roam wherever they want, even in sterile areas, and without prior screening. Giving workers open access to a sterile area is like installing an expensive home security system but leaving your backdoor wide open.

This is a huge security gap. It already has been exploited for the purposes of carrying out criminal activities, and I believe that if we continue some of our Band-Aid approaches, it is only a matter of time before those who wish to do us harm will exploit this vulnerability to attack our nation.

So it is the same thing that I started out with, is that we must be diligent.

We have now a wonderful combination before us, a representative of a very, very large airport but one, Ms. Stover, where we still

have the images of airport employees with their hands in the air or hands behind their back, who perpetrated this whole drug activity, certainly, maybe right in our eyesight but, certainly, as legal, if you will, employees of that airport.

I am reminded every time I land of the appearance of, if you will, laxness on the apron part of the airport. For the airlines that I travel on, please note that I keenly look out the window as we are, if you will, taxiing, and it is literally a small city. The appearance is that it is clearly laissez-faire, the goings and comings of individuals, deliveries, those who are giving direction, trucks driving back and forth. So it looks like an exposed area.

And I think, Mr. Principato, you would be concerned, as your directors should be concerned, about that exposure.

So my questions will be to see if we can get this sense of urgency, and although we want convenience and although we want to have a legislative initiative, I know the Senate has a bill, that balances interests, I said once that we cannot opt for bucks, dollar bills, over security. That goes to the whole wave of foreign ownership, it is okay because we are getting a buck. We have to look at how our ports are managed, even if we think it is in vogue to have foreign ownership or maybe it is not only in vogue but it is really the norm.

The same thing with our airports. There are reasons to have convenience, because our traveling public is looking for fastness, but I would think that we also want security. We have got Mr. Holden here who has come out of the private sector, his company is in the private sector, and some airport, thought enough of the breach to engage Mr. Holden's company.

So let me start with Mr. Principato to talk about TSA's plan, if you have not answered that. And when I say, talk about the plan, there are a lot of good elements to it. This week is dominated by Virginia and I am very sensitive. I think I mentioned in another committee that members are tempered in their actions. You will see us probably move swiftly in the weeks to come, but we are tempered because of the mourning. But the point is, is that we now know we have another element to bad acts behavior.

Give me a sense of the urgency of your organization about moving quickly and whether or not this behavioral concept that now is glaringly before us in light of the horrific tragedy of Virginia Tech, where are you all going and what is your assessment of what TSA has begun to do?

Mr. PRINCIPATO. We have been working very closely with TSA on these concepts. ACI, AAAE and other organizations have been working very closely with TSA on these concepts and developing them.

Let me say that, as I said earlier in my statement, airport directors and their staffs feel that sense of urgency every day. I get calls from our members from airport directors every day about all matter of things, but three-quarters of them—I keep track—three-quarters of them are about security and they are working day after day after day to improve the security at their airport.

Professionals like Ms. Stover, who is sitting next to me here, working with her director, you mentioned Rick Vacar before and

Mr. Mancuso down there, working very hard to increase the security at their airports.

And we believe that you can never stand still, that you can never say, "We are done. We have got the most secure system, we are done. We can't do anything more."

Which is why I am very excited about working with TSA on some of these concepts and rolling them out and trying to make sure that—testing them out, see what works, what doesn't work, what kind of combinations work and get the best possible system put in place, knowing that once we do that, we are going to keep at it, we are going to have to keep adjusting, we are going to have to keep changing, and we are never going to be able to go to sleep on this. This is something we have to do every day, and our members feel that acutely.

Ms. JACKSON LEE. Do you feel that you should move faster on this and should be moving more quickly now?

Mr. PRINCIPATO. I will say that that sense of urgency is there every single day, and, certainly, a discussion like this helps focus the mind.

Ms. JACKSON LEE. I will do to myself what I have done to a variety of members and yield myself an additional—I ask to yield myself an additional 3 minutes. Any objection?

Ms. Stover, you do 100 percent screening at Miami. As I said to you, the images are still very prominent in our minds about the incident that occurred, one of the first more glaring incidents, others probably are occurring without newsworthiness. Orlando represents another one.

You do 100 percent screening. What are your challenges? Why can't we implement the 100 percent screening and look closely at the apron of the airport? What a large airport you are addressing that question. Do you think you have gotten your hands around the apron aspect by the fact that you are screening 100 percent of the persons that are there?

Ms. STOVER. What we do today, quite frankly, won't be good enough for me tomorrow. We are getting our handle on this. I think more so than anything else, it is a deterrent from any type of illegal activity.

Yes, we can implement 100 percent screening, and I am encouraged at the discussion. I know some airports are nervous about it, but, certainly, at Miami, we have intercepted firearms, we have intercepted stolen computers, large sums of cash and other items that were stolen. And I am proud of that program, and it took a lot of pain to get where we are at. And we got there based on a thoughtful approach of working with the airlines and the unions to incrementally reduce the access points.

We didn't do it overnight; we did it in phases. So that where we are at today, only four access points with workers, five elevators that the guards there searching your personal effects. I am still not comfortable. I am still not comfortable about the insider threat, and a lot of that is because of the background checks.

I won't get into too many details in a public forum, but the NCIC is more so the name-based background and fingerprints are more accurate, and I would like to know these airport workers that have been in our country for only a year. I don't know if they are per-

sons of interest in international locations, and that is a disconnect that I would like to see the industry and TSA and members of Congress work more toward getting more expanded background and credentials.

It doesn't necessarily prohibit an act like such happened at Virginia Tech the other day with a person whose prints came up clean and they basically went in and committed this massacre, but it is all a part of the discussion.

Ms. JACKSON LEE. Well, as we are ongoing in our thinking, remember, we mentioned behavior, and, certainly, that might have been an element that would have been very, very important in the assessment of the tragedy of Virginia Tech.

Certainly, not knowing someone is being a person of interest and fingerprints being clean, but this tragedy of mental health issues but other behavior issues that may not be attributable to mental health, still, that may be another element, which is one of the things TSA has mentioned.

Ms. STOVER. Correct. And TSA could possibly think about rolling out a behavior program for airport security directors or the airport directors, a train the trainer type of approach. They are using SPOT, I am using Rafi Ron, who is the originator of the methodology. He has trained a core group of my police officers, and then I went to them and said, "Okay, now you need to train us."

So we have a partnership on this and we are doing it, and we are now instituting a new directive that will require every airport worker who is going to get a badge or renew their badge to go through the training. So it will be woven into the fiber of the security program.

Ms. JACKSON LEE. Well, you heard me say as I started this hearing that we were going to have a series of hearings on a large number of airport security issues. Do you think that is a relevant approach to take?

Ms. STOVER. As a representative of the airports, yes, I do.

Ms. JACKSON LEE. Mr. Holden, thank you so very much and thank, if I might, the familia, Gerry, for making the accommodation to us. Tell us what you believe you have accomplished in Orlando. Again, that was a glaring news-focused breach, and I indicated that there are so many products that are provocative that employees have access to, one of which, which is conspicuous, would be weapons. Tell us how you believe you have worked your way into the system of airports and provided a service.

Mr. HOLDEN. Well, I will charge into the airlines and the airports. Specifically, it started in San Francisco, and we did that by assembling a team with airline background. We have been able to work with the TSA, with the airport authorities, with the FSDs at these airports to ensure that we are following all the guidelines and mandates that are set forth by the TSA.

This cannot be accomplished by a company or a team alone. It has to be a team approach. And every airport that we go to our approach is to become a part of the team, to become a part of the family. And as we do these things and get lessons learned, we are able to increase where we stand in security.

We make it a point to educate our employees on the need for security and the rules of security. We also go another step to make

sure that we do not allow Bill Holden to work the same location every day. We think the movement of employees is very important.

You asked about Orlando. We are able to work with the team in Orlando by, one, we have a history of being able to assemble, in a short timeframe, a number of employees to do the job, but we go a step further. It was mentioned earlier about background checks. In some areas that we have ventured, we are finding employees who had background checks who we have had to term, if I can use that, because of false location of background checks. This is one of the biggest challenges that we have is to make sure that background checks are thorough.

Not only do we perform a background check using the standard methods, but we have in place a process wherein that we meet all employees to question the employees. We have a very extensive checklist to make sure that we try to capture with each new hire or each incumbent employee anything in the background that may be service that would not ordinarily allow that person to work.

So working with the airports as a team, working with FSD as a team, working with the airport community as a team helps us succeed in what we are doing as far as security.

Ms. JACKSON LEE. Did you use Miami as a model or did you create a new model? Is there any enhanced technology that you have that you are utilizing?

Mr. HOLDEN. We use Miami's history as a model. We use the information that we have in ADASP, and we also use our past experience with other security that we have performed outside of the airport community.

Ms. JACKSON LEE. Do you believe that it is important, as you look at airports across the country, San Francisco, Orlando, that continued assessment of the security concerns at airports is an important responsibility or challenge for this committee? Should we continue to have oversight over new and different ways to improve the security of airports and of course airlines and the traveling public?

Mr. HOLDEN. After the events of 9/11, my concerns with airport security was as we move further down the road from airport security that changing face that we apply to airport security on 9/11 will soon fade away. Without oversight of airport security, we will be back to the point we were prior to 9/11. We need to dedicate the resources to ensure that we do not go back to the events prior to 9/11 and changing the face of security. We have got to continue to build on what we have and what we have accomplished and not lose sight of the fact that airport security is and should be strong.

Ms. JACKSON LEE. Mr. Principato, I am going to let you answer, but let me yield first to the very patient distinguished gentleman from Colorado—

Mr. PERLMUTTER. I have already gotten to speak. I thought this chairman was—

[Laughter.]

Ms. JACKSON LEE. All right. It is good to be able to have colleagues in the same class salute each other.

Then that means I can yield to Mr. Principato. Thank you.

Mr. PRINCIPATO. Thank you. Just very quickly, and maybe not to differ entirely from what Mr. Holden said, of course, I think there

is a proper role for the oversight of this subcommittee and the Congress, and we welcome that.

I don't think we are ever going to—

Ms. JACKSON LEE. Say that again, Mr. Principato.

Mr. PRINCIPATO. There is certainly a role for the oversight of the Congress and this committee and this subcommittee, and we welcome that, but I don't think we are ever going to go back to the mindset, the pre-September 11, 2001 mindset. I think we are cured of that. I don't think that is going to happen. You certainly have the pledge of this organization and our members that that is not going to happen, but we do certainly welcome that oversight and the ability to work with you.

Ms. JACKSON LEE. As I close this hearing, I am going to play a game show a little bit and ask each of you to give just one issue of security that you think we should, going forward, be cognizant.

Ms. Stover, you had mentioned something toward the end of your testimony, I don't know if you remember that, and you might repeat it, but you were saying something needed to be expanded, and I am sorry that I didn't catch it, but you may have a new idea as we go to the three of you, as I close the hearing.

Ms. STOVER. Okay. Well, you are asking me to pick one that I think is the most important.

Ms. JACKSON LEE. And you won't be limited to that. We will have you back.

Ms. STOVER. Oh, thank you.

I think the credentialing and the background checks are critically important to revisit, and, of course, we are a proponent of the employee screening. We would like to see that woven into your legislation if it is done with the thoughtfulness of the configuration of each of the airports. And then, lastly, behavior pattern recognitions, because we were the first airport to lead the way on that, so I have to say that.

Ms. JACKSON LEE. And you are still going strong.

Ms. STOVER. Oh, absolutely. And no one is going to get their ID back unless they go through my 2-hour course.

Ms. JACKSON LEE. Mr. Principato?

Mr. PRINCIPATO. I am going to agree with everything Lauren just said and add, as I said in my discussion with Congressman Perlmutter before, the movement from a labor-intensive to a technology-intensive security system, making greater use of technology, for example, inline EDS systems, which will make the security—

Ms. JACKSON LEE. Pardon me?

Mr. PRINCIPATO. Inline EDS, which will make the security system much more efficient and much more secure and allow us to better utilize those scarce resources.

Ms. JACKSON LEE. Thank you.

Mr. Holden?

Mr. HOLDEN. We have benefited greatly from technology. With everything good sometimes come things bad, so I have to agree with my distinguished colleague, credentialing and background checks. Technology has helped the bad boys, if you can call them that, to breach security with false ID. So credentialing and background checks is very, very important.

Ms. JACKSON LEE. Thank you very much.

This Congress is at a crossroads, the committee is at a crossroads. That is to be able to match the major function of airports, the traveling public, with the new era in which we find ourselves, not in this country, but in this world. Having been to a number of borders, northern border, southern border, Europe, if you will, and the third border, we find out that areas that are surrounding the United States are also part of the story of security.

This committee will look both nationally and internationally as we look at the traveling public and ways of providing security. We will need the cooperation of the Airports Council, we will need the cooperation of major and small airports around the nation and frankly the world.

And, Mr. Holden, we certainly are hopeful that there will be transparent contracts rendered by airports and the Department of Homeland Security and they will be effective partners, as we know that Orlando believes that you have been, your company has been, to be able to provide us security. The only way we can get past the crossroads is that cooperative spirit and information.

This committee may submit to the members additional questions. We would ask that you would expeditiously submit those questions back to us. We expect that will have the opportunity to have a markup shortly, and as we do so, we will be cognizant of the work that each and every one of you have done.

So I thank you for the valuable testimony, and I thank the members for their questions and their insight. We usually have a vigorous markup. I know there will be a number of amendments that will reflect the different viewpoints of members, but we will cite airports that have 100 percent screening of their employees, and we will make the point that their doors are still open.

And so we can find ways to accommodate our friends, pilots, flight attendants and others, but we will make sure that we move forward on the challenge that we have of securing America.

Hearing no further business, the subcommittee stands adjourned.

[Whereupon, at 1:50 p.m., the subcommittee was adjourned.]

FOR THE RECORD

PREPARED STATEMENT OF THE HONORABLE GINNIE BROWN-WAITE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

I am in complete support of Congresswoman Nita Lowey's bill, H.R. 1413. The bill's purpose, to "direct the Assistant Secretary of Homeland Security (Transportation Security Administration) to address vulnerabilities in aviation security by carrying out a pilot program to screen airport workers with access to secure and sterile areas of airports," is something our nation desperately needs to secure our airports. I also have a submission I would like to put in to the record from the Orlando Aviation Authority on this subject.

Recent events that took place at the Orlando International Airport are a case in point.

The arrest last month of various airline employees attempting to smuggle 13 handguns and 8 pounds of marijuana aboard a flight from Orlando International Airport to San Juan, Puerto Rico, is a perfect example of a striking gap in airline security nationwide.

Specifically, the fact that airline employees are not required to go through the same security checkpoints as other passengers leaves a huge gap in our aviation security system. Given that an employee was willing to take the risk of smuggling illegal weapons and drugs onto a flight for a few thousand dollars would certainly lead one to believe it plausible that an employee of an airline could be bribed by well financed terrorists to obtain access to an airport's infrastructure.

On March 12th I met with TSA officials and Members of the Greater Orlando Aviation Authority at the Orlando airport. Together, we reached an agreement that the airport would provide 1005 screening of all Orlando International Airport employees, baggage and passengers.

Miami International Airport already has a program which screens every worker, and there is no reason why Orlando, or in fact, all airports nationwide, should not be conducting the same type of security measures.

For Florida, tourism and travel form the backbone of Florida's economy, and obviously, those traveling to the state need to feel safe during their commute. Similarly, those traveling domestically and internationally via U.S. airports need to be secure, and increasing and enforcing security procedures for airline employees serves as an important step forward towards achieving this goal.

GREATER ORLANDO

AVIATION AUTHORITY

TESTIMONY BY

THE

GREATER ORLANDO AVIATION AUTHORITY

HEARING ON

AIRPORT SECURITY: THE NECESSARY IMPROVEMENTS TO

SECURE AMERICA'S AIRPORTS

April 19, 2007

Before The subcommittee on Transportation Security and Infrastructure Protection

Committee on Homeland Security

Thank you for the opportunity to comment on HR 1413. Your leadership in promoting safety and security for the traveling public is appreciated by airports across the United States.

Our goal is to work in cooperation with the Department of Homeland Security and State and local law enforcement agencies to ensure the safety and security of passengers traveling through Orlando International Airport.

Attached you will find a recent presentation approved by the Greater Orlando Aviation Authority Board. This presentation lays out in detail the Authority's plan to screen employees with access to secure and sterile areas of the airport.

The Authority is funding $1.8 million in additional equipment costs and an additional $3.2 million in personnel costs for a total of $5 million during the first year of this program. The cost of this program will place a burden on an already constructed budget.

VerDate Nov 24 2008 07:47 Jun 15, 2009 Jkt 000000 PO 00000 Frm 00049 Fmt 6633 Sfmt 6621 H:\DOCS\110-HRGS\110-25\43561.TXT HSEC PsN: DIANE

Attachment:

Enhanced Employee

Screening

The Plan

1. Reduce Access
2. Add Technology
3. Enhance Employee Screening

Enhanced Employee Screening

BAGGAGE MAKE-UP TO BAGGAGE CLAIM DOORS

1. TSA to provide screening at these doors ( ) under interim agreement
2. GOAA to provide additional Customer Service Representatives on a 1 to 1 basis

Projected additional cost: $1 million

Enhanced Employee Screening

VEHICLE ENTRY CHECKPOINTS

Emergency Purchase Order with Covenant AviationSecurity
- TSA Certified Company
- Training to be provided by Lockheed Martin
- Mobile force can be expanded to other locations
- Immediate start up

Projected additional cost: $2.2 million

Enhanced Employee Screening

- Add additional security equipment
- Fixed and mobile assets
- State and Federal procurement lists will be used

Projected additional cost: $1.8 million

Funding for Implementation:

1. Equipment costs from 1997 Revenue Bonds	$1.8 million
2. Personnel costs from Operations and Maintenance Fund	$3.2 million
Total:	$5.0 million
3. Possible federal & pilot program appropriations	

Greater Orlando Aviation Authority

Wednesday, March 21, 2007