ACCESS CONTROL POINT BREACHES AT OUR NATION'S AIRPORTS: ANOMALIES OR SYSTEMIC FAILURES?

HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION SECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

MAY 16, 2012

Serial No. 112–91

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE
78–151 PDF WASHINGTON : 2013

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

COMMITTEE ON HOMELAND SECURITY

Peter T. King, New York, *Chairman*

Lamar Smith, Texas
Daniel E. Lungren, California
Mike Rogers, Alabama
Michael T. McCaul, Texas
Gus M. Bilirakis, Florida
Paul C. Broun, Georgia
Candice S. Miller, Michigan
Tim Walberg, Michigan
Chip Cravaack, Minnesota
Joe Walsh, Illinois
Patrick Meehan, Pennsylvania
Ben Quayle, Arizona
Scott Rigell, Virginia
Billy Long, Missouri
Jeff Duncan, South Carolina
Tom Marino, Pennsylvania
Blake Farenthold, Texas
Robert L. Turner, New York

Bennie G. Thompson, Mississippi
Loretta Sanchez, California
Sheila Jackson Lee, Texas
Henry Cuellar, Texas
Yvette D. Clarke, New York
Laura Richardson, California
Danny K. Davis, Illinois
Brian Higgins, New York
Cedric L. Richmond, Louisiana
Hansen Clarke, Michigan
William R. Keating, Massachusetts
Kathleen C. Hochul, New York
Janice Hahn, California
Vacancy

Michael J. Russell, *Staff Director/Chief Counsel*
Kerry Ann Watkins, *Senior Policy Director*
Michael S. Twinchek, *Chief Clerk*
I. Lanier Avant, *Minority Staff Director*

SUBCOMMITTEE ON TRANSPORTATION SECURITY

Mike Rogers, Alabama, *Chairman*

Daniel E. Lungren, California
Tim Walberg, Michigan
Chip Cravaack, Minnesota
Joe Walsh, Illinois, *Vice Chair*
Robert L. Turner, New York
Peter T. King, New York *(Ex Officio)*

Sheila Jackson Lee, Texas
Danny K. Davis, Illinois
Cedric L. Richmond, Louisiana
Vacancy
Bennie G. Thompson, Mississippi *(Ex Officio)*

Amanda Parikh, *Staff Director*
Natalie Nixon, *Deputy Chief Clerk*
Vacant, *Minority Subcommittee Lead*

CONTENTS

Page

STATEMENTS

WITNESSES

PANEL I

PANEL II

ACCESS CONTROL POINT BREACHES AT OUR NATION'S AIRPORTS: ANOMALIES OR SYSTEMIC FAILURES?

Wednesday, May 16, 2012

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

The subcommittee met, pursuant to call, at 10:03 a.m., in Room 311, Cannon House Office Building, Hon. Mike Rogers [Chairman of the subcommittee] presiding.

Present: Representatives Rogers, Lungren, Walberg, Cravaack, Turner, Jackson Lee, Thompson, Davis, and Richmond.

Mr. ROGERS. The Committee on Homeland Security, Subcommittee on Transportation Security will come to order. The committee is meeting today to receive testimony on secure area access control points at our Nation's airports.

I would like to welcome everybody to this hearing and thank our witnesses. We look forward to your testimony and greatly appreciate the time and effort that you had to put into preparing for these hearings.

Securing our Nation's aviation system requires 100 percent accuracy. Our enemies could exploit any weaknesses in the system.

The many reports of security breaches and unauthorized access to the tarmac are extremely troubling and continue to underscore the need to strengthen our access controls.

We must make certain that the billions of taxpayer dollars we spend screening passengers is not wasted if systematic vulnerabilities exist through the back doors of our airports that could lead to attack.

I look forward to questioning TSA and its partners about the measures in place to not only physically protect our airports, but also to ensure that employees with sterile-area access have been thoroughly vetted and do not pose a threat.

A secure airport requires the coordination and cooperation of a range of stakeholders. When a breach occurs, it is incumbent on both TSA and its partners to evaluate what went wrong and take immediate steps to mitigate or eliminate the vulnerability.

What concerns me is that we had such a large number of breaches occurring, it is hard to believe that these do not reflect some larger systematic problem.

In October 2011, a local news station in Atlanta investigated the access control procedures at Atlanta International Airport after a whistleblower contacted the station.

The whistleblower, an employee of an airline catering company, was able to capture on video a company employee swiping his badge to let another person in a secure area, allegedly without that person having the necessary credentials to pass through.

The video also revealed that an employee was able to put unauthorized juice containers onto several carts as inspectors from the company responsible for inspecting all food containers loaded onto an aircraft, stood nearby without doing anything.

The Aviation and Security Transportation Security Act requires all supplies put on an airplane to be sealed to ensure easy visual detection of tampering. However, the video showed rows of unsealed catering carts on the dock and in trucks waiting to be loaded onto flights.

While we can all hope that this is an isolated incident at Atlanta Airport, this is more than likely indicative of a broader, more pervasive problem affecting airports Nation-wide.

In another recent case, a civilian vehicle crashed through an airport gate and drove onto a taxiway near a busy runway at Philadelphia International Airport. According to sources, the vehicle drove past a Philadelphia police officer in a patrol car and two airport employees.

Thankfully in these two examples there was no harm done. However, we may not always be so lucky. With a huge financial cost to taxpayers, we frankly expect better from TSA and others who are responsible for securing our aviation system.

Finally, I cannot stress enough how disturbing it is that DHS and the Office of the Inspector General reported just this week that over half of all security breaches that occur at airports are never properly reported to TSA headquarters. In addition, only half of all incidents result in some corrective action.

Mr. Sammon, these are sobering findings.

I am eager to receive testimony today from the acting DHS IG about the report and the recommendations that TSA will need to address going forward.

With that I now recognize the Ranking Member of the full committee, the gentleman from Mississippi, for any opening statement he may have.

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

No agency in the Federal Government has a more central role in securing our aviation system than TSA. Accordingly, it is essential that TSA have the necessary processes and protocols in place to secure our aviation systems.

These processes and protocols must include ensuring the integrity of airport perimeters by securing access controls and providing comprehensive and sufficient guidance to airport operators.

In March, the media reported on an individual who drove a truck onto the runway at the Philadelphia Airport. Last year, we learned of the tragic case of a young man who breached the airport perimeter and became a stowaway in a wheel well of a plane.

While none of these people involved in these cases had any terrorist intentions, each case should have been put on notice that the grounds surrounding the airport must be considered in airport vulnerability assessments.

To accomplish that, TSA must establish a single comprehensive definition of what constitutes a security breach. Failing to establish such a definition leads to inconsistent and subjective reporting.

Without a clear understanding of the types of breaches occurring at our airports, TSA cannot make any reasonable conclusions about the kinds of security enhancements that should be broadly implemented. But in a system of layered security, perimeter security must be complemented with other measures.

An equally important component of layered security environment is ensuring that only properly vetted people can gain access to the secured areas of the airport and access to aircraft and field operations. The vetting process should not be a burden to individuals or businesses, but it must enhance the security of the airport.

I look forward to hearing from our second panel of witnesses on how TSA's vetting process is working today.

Mr. Chairman, thank you for holding this hearing, and I yield back.

Mr. ROGERS. I thank the gentleman.

Other Members of the committee are reminded that opening statements may be submitted for the record.

We are pleased today to have several distinguished witnesses before us on this important topic. Let me remind the witnesses that their entire written statements will appear in the record.

Our first witness, Mr. John Sammon, currently serves as assistant administrator for the Office of Security Policy and Industry Engagement at TSA. We appreciate Mr. Sammon for appearing once again before this committee.

The Chairman now recognizes Mr. Sammon for his opening statement.

STATEMENT OF JOHN P. SAMMON, ASSISTANT ADMINISTRATOR, OFFICE OF SECURITY POLICY AND INDUSTRY ENGAGEMENT, TRANSPORTATION SECURITY ADMINISTRATION

Mr. SAMMON. Good morning Chairman Rogers, and Mr. Thompson, and the distinguished Members of the subcommittee. I appreciate the opportunity to appear before you today to discuss the Transportation Security Administration's responsibility regarding access control at U.S. commercial airports.

Every airport and airline has a security plan of which access control is an important piece. While TSA is responsible for approving the plan and inspecting airport compliance with the plan, airport authorities and airlines are responsible for carrying out the plan.

TSA sets standards, conducts inspections associated with access control including badging, perimeter security, and testing of access control processes at airports.

TSA analyzes the results of these inspections and assessments to develop mitigation strategies that enhance an airport security posture and to determine if any changes are needed. Every commercial airport receives an annual security inspection to include an assessment of perimeter and access controls.

While the current badging process was put in quickly after 9/11 thanks to the work of AAAE, TSA, and the Nation's airports, TSA issued security directive 1542–08G in 2009 to address a number of badging process deficiencies to include identity verification and work authorization, document authentication, standardized 2-year badge renewal requirements, requirements to return and reactivate expired badges, recordkeeping requirements, documentation requirements for naturalized and non-U.S. citizens, enrollment process audits, and expanded the covered populations.

While that directive improved the badging process, TSA has written a regulation called the Universal Rule that addresses many of the gaps left by that security directive, and also concerns that have been raised by the DHS inspector general.

Specifically that rule will provide for trusted enrollment agents to identify verification and document inspection and collection; more uniform, more stringent, and recurrent training for enrollment agents; one uniform enrollment process; data that will be entered directly into the TSA system for adjudication; TSA up-front edits for completeness and accuracy of data; identity documents scanning the TSA; identity documents verification by TSA; criminal history records check every 5 years which is consistent with other Federal background checks; strengthen ID verification and immigration standards, including documentary evidence of U.S. citizenship.

It will be a person-centric versus an airport-centric system—enroll once and use many times in different fields. Instant access to the data by TSA inspectors, and it will be much more enforceable than what we have today.

That rule is currently being reviewed within the administration, and we hope to issue it for comments later this year. In the mean time, TSA will be stepping up inspection efforts to close gaps in existing process.

In terms of breaches, the DHS inspector general recently released a report on airport breaches. That report had two recommendations.

The first was to define and use one comprehensive definition of what constitutes a security breach, and ensure the guidance is clearly understood and used throughout the agency. The second recommendation was to develop a comprehensive oversight program for reporting and corrective actions.

TSA concurred with the recommendations, and the inspector general found that TSA's planned actions sufficiently addressed the two recommendations in this report.

TSA's goal is to work with airport authorities and airlines in our shared responsibilities to stay ahead of evolving terrorist threats while protecting passengers' privacy and facilitating the efficient flow of travelers and legitimate commerce.

TSA's airport control initiatives are one part of that comprehensive effort.

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

[The statement of Mr. Sammon follows:]

PREPARED STATEMENT OF JOHN P. SAMMON

MAY 16, 2012

Good afternoon Chairman Rogers and Ranking Member Jackson Lee and distinguished Members of the subcommittee. Thank you for the opportunity to testify today about the Transportation Security Administration's (TSA) successes and challenges in developing and implementing a comprehensive risk-based approach to secure our Nation's transportation systems, including the management of airport access controls. In 2011, the Transportation Security Administration's 50,000 Transportation Security Officers screened more than 603 million passengers at 450 airports across the country and stopped more than 125,000 prohibited items at airport checkpoints. Of those items, more than 1,300 were firearms.

TSA employs risk-based, intelligence-driven operations to prevent terrorist attacks and to reduce the vulnerability of the Nation's transportation system to terrorism. TSA protects the Nation's transportation systems to ensure freedom of movement for people and commerce. TSA's security measures create a multi-layered system of transportation security that mitigates risk. In partnership with airport operators, airlines and local law enforcement agencies, TSA secures our Nation's commercial airports through a variety of programs that create layers of security. These measures include a focus on preventing and detecting the unauthorized entry, presence, and movement of individuals and ground vehicles into and within the Airport Operations Areas (AOA) and the secured area of an airport.

RISK-BASED SECURITY

TSA is committed to focusing resources on higher-risk aviation passengers, while speeding the travel of lower-risk populations, and we have made significant progress transforming TSA's approach to aviation security away from a one-size-fits-all paradigm. We continue to evolve our security approach by examining the procedures and technologies we use, how specific security procedures are carried out, and how screening is conducted.

TSA's risk-based and intelligence-driven Security Playbook program strengthens the transportation security environment by increasing unpredictability and providing additional layers of security. This program employs security measures at direct access points and airport perimeters and uses a variety of resources and equipment to conduct screening of individuals and vehicles entering the AOA. Examples of the security measures that may be employed at direct access points and airport perimeters include: Vehicles inspections, explosive trace detection (EDT) of individuals and property, enhanced screening, accessible property searches, and ID/media verifications, as well as behavior detection.

Following are some of the concrete steps we have taken to implement key components of the agency's intelligence-driven, risk-based approach to security, advancing the agency toward the ultimate goal of becoming a high performing counterterrorism agency that provides the most effective security in the most efficient way possible.

KNOWN CREWMEMBER

We hold airline pilots responsible for the safety of the traveling public every time they fly a plane. It makes sense to treat them as our trusted partners. To build on our risk-based approach to security, we are currently conducting a pilot where TSA security officers positively verify the identity and employment status of airplane pilots, which enables the pilots to receive expedited access through the checkpoint. The Known Crewmember program is the result of a collaborative effort between the airline industry, pilots, and TSA, which currently allows uniformed pilots from 28 airlines in ten airports to show two forms of identification. After evaluating operational data from ten airports, and through much discussion with industry representatives, we are planning to expand the Known Crewmember solution to more airports this calendar year.

TSA PRECHECK EXPEDITED PASSENGER SCREENING

Perhaps the most widely known risk-based security enhancement we are putting in place is TSA PreCheck™. Since first implementing this initiative in the fall of 2011, the program has been expanded to 14 airports and over 1,000,000 passengers around the country have experienced expedited security screening through TSA PreCheck™.

Under TSA PreCheck™, travelers volunteer information about themselves prior to flying. TSA pre-screens TSA PreCheck™ passengers each time they fly through participating airports. If the indicator embedded in their boarding pass reflects eligibility for expedited screening, the passenger is able to use the TSA PreCheck™ lane. TSA PreCheck™ travelers are able to divest fewer items, which may include leaving on their shoes, jacket, and light outerwear, and may enjoy other modifications to the standard screening process. As always, TSA continues to incorporate random and unpredictable security measures throughout the security process, and at no point are TSA PreCheck™ travelers guaranteed expedited screening.

Currently, eligible participants include certain frequent flyers from Alaska Airlines, American Airlines, and Delta Air Lines, as well as existing U.S. citizen members of U.S. Customs and Border Protection's (CBP) trusted traveler programs, such as Global Entry, flying domestically on participating airlines. TSA is actively working with other major air carriers to expand both the number of participating airlines and the number of airports where expedited screening through TSA PreCheck™ is provided. In February 2012, Secretary Napolitano and TSA Administrator Pistole announced the goal to have TSA PreCheck™ rolled out and operating at 35 of the busiest domestic airports by the end of 2012.

TSA has expanded the TSA PreCheck™ population to include active duty U.S. Armed Forces members with a Common Access Card (CAC) traveling out of Ronald Reagan Washington National Airport. Similar to other PreCheck™ travelers, service members always undergo the standard TSA Secure Flight pre-screening. If we are also able to verify the service member is in good standing with the Department of Defense, by scanning their CAC card at the airport, they will receive TSA PreCheck™ expedited screening benefits.

CREDENTIAL AUTHENTICATION TECHNOLOGY/BOARDING PASS SCANNING SYSTEM

TSA is also employing technology to automatically verify boarding passes, and provide TSA with a greater ability to identify altered or fraudulent passenger identification documents. This technology, known as Credential Authentication Technology—Boarding Pass Scanning Systems (CAT–BPSS), will eventually replace the current procedure used by security officers to detect fraudulent or altered documents. CAT–BPSS enhances security and increases efficiency by automatically comparing a passenger's ID and boarding pass to a set of security features to concurrently seek to identify indicators of fraud and ensure that the information on both documents match. The system can screen a wide range of travel documents. TSA began testing the technology in July 2011 and has begun evaluations at select airports.

STRENGTHENING ACCESS CONTROL

Effective access control at our Nation's airports is vital to ensure the safety of the traveling public. The regulatory compliance inspector workforce routinely conducts access control tests as directed by the National compliance work plan. Access control procedures are reviewed and tested at all areas where access may be gained to non-public areas of the airport to include the air operations area and the Secure Identification Display Area (SIDA)/Secure areas. Access control measures can range from simple lock and key control to biometric devices that may require a scan of your fingerprint or iris to make positive identification of individuals trying to gain entry into the secure airport environment. Inspectors use different methods to try and defeat or compromise various access control devices as part of their regular duties. If any weaknesses are discovered, they are communicated to the airport operator immediately so that corrective measures can be implemented.

TSA also conducts on-going and comprehensive airport inspections to enhance security and mitigate risk associated with access control and perimeter integrity, including Joint Vulnerability Assessments, Special Emphasis Inspections, and the testing of access control processes at airports. TSA analyzes the results of these inspections and assessments to develop mitigation strategies that enhance an airport's security posture, and to determine if any changes are required. TSA also works in collaboration with airport operators to identify effective best practices across the industry regarding access control and perimeter security.

CONCLUSION

Thank you for the opportunity to appear before you today to discuss TSA's efforts in securing our Nation's transportation system in the most effective and efficient manner possible.

Mr. ROGERS. Thank you, Mr. Sammon, for your testimony. We appreciate you being here today.

Our second witness is Mr. Charles Edwards. He is the acting inspector general of the Department of Homeland Security.

Mr. Edwards has appeared before this subcommittee on a range of important topics, and the Chairman now recognizes him for his opening statement.

STATEMENT OF CHARLES K. EDWARDS, ACTING INSPECTOR GENERAL, DEPARTMENT OF HOMELAND SECURITY

Mr. EDWARDS. Good morning, Chairman Rogers, Ranking Member Jackson Lee, Ranking Member Thompson, and Members of the subcommittee.

Thank you for inviting me to testify today regarding access controls at our Nation's airports. I will present the results of three audits we have conducted in the past year on this topic.

We looked at TSA's oversight of the process for determining whether an individual may be issued a badge granting unescorted access to secure areas of an airport, TSA's oversight of physical access controls at airports, and third, we looked at TSA's oversight of the reporting and collection of information about security breaches at individual airports.

We found that TSA's oversight of the process for screening employees, prior to giving them an access or security badge, did not ensure that the employees are fully screened. We analyzed data from 359 airport badging officers and identified badge holder records with omissions or inaccuracies pertaining to security threat assessment status, birth dates, and birth places.

For example, our analysis identified an individual with badges issued at three airports. Each badge showed a different birthplace.

We believe these problems exist because TSA's oversight of the process does not ensure the airports use sufficient quality assurance measures, such as checking the applications and data entry for accuracy and completeness, or provides sufficient training and tools to badge office employees.

TSA also does not require its own transportation security inspectors to verify the badge holder data during the review of airports.

We did identify several airports with best practices in the badging review process. We have provided details of those practices to TSA to share with all airports across the country.

TSA also does not require airports to conduct a recurring criminal history records check of current security badge holders. Passing an initial criminal history check does not preclude employees from engaging in subsequent criminal activity and presenting an insider threat.

For example in 2007, it was discovered that a customer service officer with no prior record had agreed to smuggle money and illegally export weapons and military equipment to a foreign country.

TSA concurred with five of our recommendations from this audit, and concurred in part with an additional recommendation.

In a separate audit we conducted covert testing to determine if unauthorized individuals could gain access to secured airport areas. Our audit identified areas of concern.

However, the detailed results of our tests are classified. We have shared the classified results with this and other appropriate Congressional committees, TSA staff, and Department officials.

The third audit looked at TSA's ability to identify and track security breaches. For the purposes of the audit, we identified an airport security breach as an individual gaining access to an unauthorized area without submitting to all screening, inspections, and detection according to TSA's standard operating procedures.

For example, a person sticking to an exit lane to get around a checkpoint would be considered a security breach. Some of the results of our testing have been designated sensitive security information and cannot be included in this testimony.

It can be stated, however, that even though TSA has several programs to report and track identified security breaches, it does not have a comprehensive oversight program to gather information about all security breaches at airports across the Nation, and therefore cannot use the information monitor trends or make improvements.

TSA does not provide needed guidance and oversight to ensure that all breaches are consistently reported, tracked, and corrected. We determined that only 42 percent of the security breaches be reviewed in individual airport files but reported to TSA's official records.

For example, a person entered through a security gate with a handwritten boarding pass, but was not reported TSA's official records as a security breach incident. Further, our review of airport records identified corrective actions being taken for only 53 percent of the security breaches in airport files.

We made two recommendations. TSA concurred with both and started taking action to implement them.

In conclusion, despite the billions of dollars spent on multiple layers of aviation security since September 11, 2001, issues remain. Our recent reports have included best practices and recommendations to address those vulnerabilities.

TSA has agreed to make changes to improve the effectiveness of its efforts to protect the traveling public.

Mr. Chairman, this concludes my prepared remarks. I thank you again for the opportunity to testify before this committee.

[The statement of Mr. Edwards follows:]

Prepared Statement of Charles K. Edwards

May 16, 2012

Good morning Chairman Rogers, Ranking Member Jackson Lee, and Members of the subcommittee: I am Charles Edwards, Acting Inspector General for the Department of Homeland Security (DHS) Office of Inspector General (OIG). Thank you for inviting me to testify today about the results of our audits regarding the Transportation Security Administration's (TSA) access controls at our Nation's airports. Since the events of September 11, 2001, TSA has spent billions of dollars on multiple layers of aviation security and relies on those layers of security to ensure the safety of the traveling public.

My testimony today will present the results of three recent audits of aspects of TSA's oversight of security at our Nation's airports.[1] Specifically, I will address TSA's oversight of the process to vet airport, or airport vendor, employees prior to giving them badges that allow unescorted access to secure areas; TSA's oversight of airports' physical access controls; and last, I will summarize our evaluation of

[1] The information provided in this testimony is contained in the following reports: *TSA's Oversight of the Airport Badging Process Needs Improvement* (OIG–11–95); *Covert Testing of Access Controls to Secured Airport Areas* (OIG–12–26); and *Transportation Security Administration's Efforts To Identify and Track Security Breaches at Our Nation's Airports* (OIG–12–80).

TSA's collection of security breach information which should be used to identify and correct potential vulnerabilities.

AIRPORT BADGING PROCESS[2]

We evaluated TSA's oversight of the process for issuing airport security badges. These badges allow an individual unescorted access to secure airport areas, including:

- *Sterile Area.*—A portion of an airport, defined in the airport security program, that provides passengers access to boarding aircraft, and to which the access is generally controlled by TSA through the screening of persons and property.
- *Air Operations Area (AOA).*—A portion of an airport that includes aircraft movement areas, loading ramps, and safety areas for use by aircraft.
- *Security Identification Display Area (SIDA).*—A part of the AOA regularly used to load cargo on, or unload cargo from an aircraft. TSA can designate all or portions of the AOA as SIDA.

As of the time of our audit fieldwork, there were approximately 890,000 individuals with 1.2 million active badges that had access to secure areas of airports.[3]

Applicants for these badges are required to undergo a fingerprint-based criminal history records check and have an approved security threat assessment (STA) from TSA before receiving a badge and obtaining unescorted access to secure airport areas. The STA is accomplished by comparing an applicant's information against critical data sets to discern whether the applicant is a threat to transportation or National security.

TSA relies on designated airport operator employees as trusted agents to perform the essential functions of the badging process. Their duties consist of collecting, verifying, and inputting applicant data used for the STA process and fingerprinting applicants for the Criminal History Records Check. Airport operator employees are responsible for ensuring that the badge application is complete with the required biographical and fingerprint data for the STA. Critical data processed from the application includes full legal name, date of birth, place of birth, passport number, and alien registration number. Airports are responsible for ensuring that badges are issued only to qualified applicants, and must account for and manage all active and deactivated badges.

TSA has the statutory responsibility for requiring individuals with unescorted access to secure areas of the airport to be properly vetted, or checked. TSA fulfills this responsibility through its Threat Assessment and Credentialing adjudication service, which completes the STAs for applicants and provides oversight of the airports' processes through its Transportation Security Inspectors.

Individuals who pose a threat to airport security may be able to obtain badges and gain access to secured airport areas. We evaluated a database of information on active badges at 359 airports. We identified a number of badges issued with one or more instances of omissions or inaccuracies of key applicant data used for vetting, such as STA status, birthdates or birthplaces.[4] Many of the omissions or inaccuracies pertained to critical information used for vetting. For example, one applicant was listed as having three active badges at three different airports. The applications for this individual reflected three different places of birth: The United Kingdom, Ukraine, and the United States. With inaccurate information on place of birth, TSA was unable to accurately vet the applicant, yet the three airports issued the requested badges.[5]

We believe these problems exist because the design and implementation of TSA's oversight of the application process is limited. Specifically, the agency did not ensure that airport operators have quality assurance procedures for the badging application process; ensure that airport operators provide training and tools to designated badge office employees; and require its TSA Inspectors to verify the airport data during their reviews.

Quality assurance.—TSA does not ensure that airport operators have quality assurance procedures to safeguard the completeness and accuracy of the vetted data. For example, TSA does not require, and most airports do not have, different individuals verifying the entry of an applicant's information into the vetting process. Hav-

[2] *TSA's Oversight of the Airport Badging Process Needs Improvement* (OIG–11–95).

[3] Employees could have more than one badge if working for multiple employers at the airport or if working at multiple airports.

[4] The exact number of discrepancies we identified is Security Sensitive Information and cannot be disclosed in publicly available documents.

[5] We followed up on this individual's information. He is a United States citizen and all three badging application files contained copies of his passport identifying the United Kingdom as his place of birth.

ing separate individuals verifying the information would likely enhance the detection of missing or inaccurate information, such as a missing place of birth or a transposition in a date of birth.

In our audit work, we found an airport that had several procedures in place that could be considered "best practices," such as conducting on-site badge audits annually; using a supervisory review checklist to ensure that at least two agents handle each application; using equipment to check identification; and using local police to run criminal investigation checks on badge applicants.

Other best practices include: (1) One airport used daily system-generated reports to identify and resolve potential problems with active badge holders; (2) another airport had a Memorandum of Understanding with U.S. Customs and Border Protection to have the agency verify all immigration documents before submitting the information to TSA for vetting; and (3) yet another airport used a supervisory review checklist to ensure that at least two agents have reviewed the application for completeness and accuracy.

Training and tools.—In addition to the lack of quality assurance procedures for gathering and inputting the applicant data, TSA also does not always ensure that airports are providing their individuals with proper training and tools. For instance, officials at 12 airports visited did not know what happens to the data once they enter it. These officials were unaware of how data entry errors or transposed numbers related to key identifying elements could create vulnerabilities, be exploited, and provide the wrong individuals access to secured airport areas.

TSA also does not ensure airport operator employees are using available tools while performing their duties. Tools such as identification document scanners, ultraviolet lights, and loupes (magnifying lenses) allow employees to more closely inspect a document, which prevents fraud. At 8 of 12 visited airports, these employees had tools available to assist in identifying fraudulent documents, but did not consistently use them. For example, at one airport, there was an identification scanner available, which reads the magnetic strip on a driver's license or State-issued ID to display its validity. One employee admitted to using the scanner only occasionally, but not using the lights and loupes at all.

Inspectors verify data.—Regarding the inspection process, TSA Inspectors review the airport badging process during inspections; however, the limited coverage does not ensure vetting information is complete and accurate. Inspectors consult TSA's Handbook and the Performance and Results Information System to use basic questions provided, along with guidance, which is based on regulatory requirements from the CFR and TSA Security Directives. The Handbook does not require Inspectors to verify the information reported to TSA to identify discrepancies with badging information. It simply indicates that the Inspector should ensure that proper documentation has been submitted and returned to the airport operator before an employee is granted unescorted access to secured areas. TSA also does not require Inspectors to review any percentage of files; therefore, inspections of badging office records may be insufficient to determine the airports' compliance with vetting process requirements.

Additionally, Inspectors do not always have direct access to the Transportation Security Clearinghouse database and are not required to compare or cross-reference records. This direct access would not only enable Inspectors to verify records for approved STAs timely and take immediate corrective action if necessary, but it would increase inspection effectiveness and efficiency.

When our audit findings were presented to airport operators, TSA officials, and Inspectors, more than 100 updates were generated, which airport operators sent to the Transportation Security Clearinghouse. We also provided a list of suspect STAs, which prompted Inspectors to take corrective action at some locations. In fact, Inspectors at one airport revealed numerous badges issued without accurate or complete vetting data and immediately revoked access pending an approved STA.

To this end, unless airport operators implement quality assurance procedures for the badging process, the data integrity and vetting results will continue to be questionable. TSA needs to also ensure that airports are providing airport operator employees with the proper training and tools to perform their assigned duties and responsibilities. Furthermore, the agency's inspection activities must be enhanced in order to identify application omissions or inaccuracies for immediate corrective action.

COVERT TESTING OF PHYSICAL ACCESS TO SECURE AREAS OF AIRPORT [6]

We conducted covert testing to determine whether TSA's policies and procedures prevent unauthorized individuals from gaining access to secured airport areas. We also identified the extent to which Transportation Security Officers, airport employees, aircraft operators, and contractors are complying with related Federal aviation security requirements. The compilation of the number of tests conducted, the names of the airports tested, and the quantitative and qualitative results of our testing are classified, or designated as Sensitive Security Information. We have shared the information with the Department, TSA, and appropriate Congressional committees.

We identified access control vulnerabilities at the domestic airports where we conducted testing. As a result of our testing, we made six recommendations to TSA. TSA concurred with three recommendations, partially concurred with two recommendations, and did not concur with one. TSA continues to conduct significant work in a number of areas to address our recommendations.

TSA'S EFFORTS TO IDENTIFY AND TRACK SECURITY BREACHES [7]

Based on a request from Senator Frank Lautenberg, we conducted an audit into the security breaches at Newark Airport reported in the media. Senator Lautenberg asked the DHS OIG to review the contributing factors that led to the security breaches, TSA's response to the breaches, and the general level of security at the airport. He also requested that we compare the incident rate of breaches at Newark to other airports in the New Jersey/New York region and comparable airports Nation-wide, and that we determine whether corrective action had been taken on the specific security incidents.

Our audit objectives were to determine whether TSA at Newark had more security breaches than at other airports; and whether TSA has an effective mechanism to use the information gathered from individual airports to identify measures that could be used to improve security Nation-wide.

Some of our results, such as the comparison of the number of incidents at Newark to other airports, have been designated Sensitive Security Information and cannot be included in this testimony.

Overall, however, we found that while TSA has several programs and initiatives that report and track identified security breaches, it does not have a comprehensive oversight program in place to gather information about all security breaches and, therefore, cannot use the information to monitor trends or make general improvements to security. We determined that only 42 percent of the security breaches we reviewed in individual airport files were reported in TSA's official record, the Performance and Results Information System (PARIS)[8] under any category. Additionally, the agency does not provide the necessary guidance and oversight to ensure that all breaches are consistently reported, tracked, and corrected. Our audit work identified corrective action being taken for only 53 percent of the breaches we reviewed.

While there are varying levels and definitions of security breaches, our audit defined "security breach" as an individual or individuals gaining access to the sterile area, specifically at the checkpoint or exit lane, without submitting to all screening, inspections, and detection according to TSA's Standard Operating Procedures. For instance, a person entering the sterile area by sneaking through an exit lane without anyone preventing the entry would be considered a security breach.

Security breaches are documented locally by TSA at each airport, and TSA staff is required to report security breaches through PARIS and the Transportation Security Operations Center (TSOC). The TSOC is expected to use this information to identify events occurring at disparate locations throughout the U.S. transportation system that could represent an orchestrated attempt to defeat or circumvent security protocols. We did not determine or evaluate how the TSOC used the information about the security breaches we reviewed.

In its response to our audit, TSA reported that it collects thousands of records of incidents and security breaches occurring at airports and other transportation facilities. The agency documents and disseminates the information to the program offices through various channels of reporting, to include the Transportation Security

[6] *Covert Testing of Access Controls to Secured Airport Areas* (OIG–12–26).

[7] *Transportation Security Administration's Efforts To Identify and Track Security Breaches at Our Nation's Airports* (OIG–12–80).

[8] PARIS is TSA's internal reporting system and official record of a security incident and it contains 33 categories of possible incidents. In our audit, we focused on incident reports in three PARIS categories—security breaches, improper/no screening, and sterile area security events.

Operations Center, the Executive Summary Report, TSA's Management Controls Program, as well as an Assessment Team that TSA formed in March 2010.

TSA concurred with both of our recommendations in this audit report and is taking action to implement the recommendations.

Mr. Chairman, this concludes my prepared remarks. I welcome any questions that you or the Members of the subcommittee may have.

Mr. ROGERS. Thank you, Mr. Edwards. I appreciate that revealing testimony.

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

Ms. JACKSON LEE. Mr. Chairman, thank you so very much. I acknowledge the Members of the committee and the Ranking Member of the full committee.

Mr. Chairman, I have been discussing TSA since early this morning, and I thank you for your indulgence, as I made my way back from a discussion on airport security.

This is a very important hearing, and I am delighted to collaborate with Chairman Rogers and the full committee on finally getting to this hearing, and particularly hearing both Mr. Sammon and Mr. Edwards together.

A little over a year ago, under the direction of the President of the United States, Navy SEALs eliminated the architect responsible for the most horrific terrorist acts against this country. Since September 11, we have made significant progress in securing our transportation system, particularly our aviation sector.

Particularly, Mr. Sammon, I made it a point earlier in my discussions that TSA has been a pivotal part of this. Certainly I consider the officers of TSA, TSOs, a crucial front-line component to the fact that we have not had a terrorist incident of catastrophic proportions on our soil.

We all know that airports and aviation—and I would add mass transit but in this instance aviation—is a keen and focused target by terrorists tragically, probably yet unborn where individuals would wish to do the American people, but even more the American system and way of life, great damage.

We must recognize and proactively address the evolving nature of the threat to aviation to protect the millions of people every year who use commercial aviation. I am told that if we assess the amount of people that TSOs have processed or that enter airports, it would be billions over the last decade, billions plus.

In 2011 alone, U.S. Air flew 730 million passengers.

Mr. Chairman, when we discuss aviation security we usually think of transportation security officers, pilots, flight attendants, and passengers. However, we must not forget those who work behind the scenes to ensure that these jets are properly stocked and maintained.

The mechanics, technicians, and operators play a critical role in the function of our aviation system. Additionally, we must not forget about the small businesses that operate at the airports.

By and large, we know great Americans, individuals who would have no interest in doing us harm. The men and women who own, operate, or work at these shops can be a helpful component to a layered security environment, but we know it takes just one person to disrupt this system.

The men and women working at our airports and board aircraft must not only have the proper training to be a part of this effort, but they must also undergo proper vetting to ensure that risks are reduced. This is an issue that Nita Lowey and myself worked on in early years about the ingress and egress and the access to the airport and, of course, concern about the perimeter of the airport.

I look forward to hearing from our witnesses today and gaining a comprehensive understanding of where we stand with access and control and perimeter security. Earlier this year, the Philadelphia International Airport was a subject of discussion after an individual drove through the airport's metal fence and headed for the runway while a plane was gearing for landing.

If we take a survey of our airports, we will see that most of them, unless they are inner city, in city airports, have perimeters that are unattended, that may be wetlands. They are quite attractive for intrusion, for piercing.

We have a challenge. We need to address this challenge head-on.

Frankly, I want to hear today in our question and answers how TSA plans to address it head-on quickly, expeditiously, and respond to the assessment made by GAO.

Unfortunately, this is not the first time an incident like this happened and has threatened passengers at an airport, the one in Philadelphia.

Just before this particular incident took place, the media reported that another couple bypassed perimeter security, headed for the runway at Philadelphia International Airport, I am sure innocently, but it happened.

Last year, the media reported on a video at Hartsfield Atlanta Airport that showed back doors being opened to allow several people through without swiping their badges and gaining access to catering carts destined to be loaded on flights.

I would say innocent acts, friend helping friend, but it cannot be tolerated. There must be zero tolerance. We have to protect the traveling public.

We all recall the infamous shutdown in Newark in 2010. I led this committee to Newark when that happened, when flight operations were shut down and thousands of members of the flying public were inconvenienced for nearly 7 hours.

Operations were halted after a man walked into the sterile area of the airport, through the exit lane and without being screened.

These are instances where perimeters and access controls were breached and caused major disruptions, and shed light on security vulnerabilities at these airports.

Unfortunately, all relevant examples are far too many to cite in the 5 minutes allotted to me today, and span across various commercial airports of all sizes.

I look forward with you, Mr. Chairman, to ensure that we continue to conduct oversight on perimeter security at our airports.

As I mentioned to you, I am also interested in looking and holding a hearing on cabin security as well so that we don't leave all of our internal airport as a plane is airborne, if you will, to passenger courage, which we know there are many courageous passengers.

As you know, Mr. Chairman, I am committed to working with you to ensure TSA improves its operational capabilities to manage access controls and perimeter security, and that it is as effective and cost-efficient as possible.

In addition, I am concerned about the badges, and the review process for determining the badges, how the badges are protected, how they are secured, how they are maintained, and whether or not we have sufficient oversight of the individual process of providing the badges.

I want to compliment Mr. Thompson for recognizing some years back of the single focus or single contractor that was engaged or responsible for providing, assessing, reviewing the badges for personnel, and to open the door for greater opportunity for other contractors or providers.

I think that helps the level of security to have more eyes looking and more technology and more techniques, and so I thank Mr. Thompson for that.

Before yielding back, Mr. Chairman, I ask unanimous consent that statements from the Association of Flight Attendants and the United Steel Workers urging TSA to include flight attendants in the Known Crewmember Program be inserted for the record.

I have repeatedly waged this issue and raised this issue, and waged it as an effort that I hope we can join in a bipartisan way. But I ask unanimous consent to place these two letters or statements into the record.

Mr. ROGERS. Without objection, so ordered.*

Ms. JACKSON LEE. Mr. Chairman, again, this is a very important hearing. Thank you and I yield back.

Mr. ROGERS. I thank the gentlelady and she is right. We also have perimeter concerns that will be the subject of a later hearing.

As you know, this hearing was called long before this IG's report came out. We knew that there were problems with the access control points, but this was very eye-opening. We didn't realize that these particular components were problems and that being the information reporting.

Mr. Sammon, in your opening statement, you made reference to the fact that you count on the airports to follow your policies and report. But my understanding from the IG's report is that these access breaches were reported by TSA local, but they just never made their way up to big TSA to PARIS for processing.

Is that not correct? Is there some failure that is not revealed in the IG's report?

Mr. SAMMON. No, no and that is why we have concurred with the IG's two recommendations in terms of having a consistent definition. A definition, that in terms of a security breach, that has to do with immediate danger and security to the airport itself, as opposed to other definitions of breaches that have one consistent definition of a breach, and have that communicated and understood by all people not only within an airport, but among airports around the country.

So we are looking at one standard definition of what a breach is——

*Documents have been retained in committee files.

Mr. ROGERS. So——

Mr. SAMMON [continuing]. And so that people can understand that.

Mr. ROGERS. So I am understanding that the 58 percent of breaches that were not reported up to PARIS were viewed by somebody at the local TSA level as not being a breach by definition?

Mr. SAMMON. That is quite possible, yes.

Mr. ROGERS. Okay. Well, let me ask, of the 42 percent that were reported according to the IG's report, only half of them had a response made.

Do you have an answer for why that occurred?

Mr. SAMMON. Again, I would go back to—with the IG's recommendations in terms of what we have concurred with them, and in terms of our plans that we are putting forward in terms of getting a uniform definition, and developing a comprehensive oversight program that is being developed right now, the IG has concurred that those are sufficient requirements in terms of their recommendations.

These two recommendations are being held open until we supply the specific documentation and the reports of exactly what we are going to do and they are holding those two recommendations open.

Mr. ROGERS. Well, it is disturbing that, regardless of definition used, that 58 percent of breaches are not being reported up to big TSA in PARIS.

I am really disturbed by the fact that a handwritten boarding pass was able to get somebody through a checkpoint.

Do you have any explanation as to how that happened?

Mr. SAMMON. I don't, but I can get you—if you would like to put a question for the record, would be happy to get the specifics on that. I would like to give you a complete answer on that specific instance.

Mr. ROGERS. I have here a directive, a 10-page document, that TSA has outlined, dated December 16, 2005, on how to report incidents to PARIS.

I would like to offer this for the record. If there is no objection, it will be submitted.*

The first thing that I am most concerned about is there is a recorded document about this. Apparently nobody was—in a directive that nobody was following or, at least, 58 percent of the time they weren't following.

Are you saying the definition outlined in your own policy is not adequate?

Mr. SAMMON. Apparently, it was not clear enough. What we are doing right now is—based upon working with the IG—is coming up with a clear set of directions and making sure those directions are understood throughout the airports that TSA operates in. Yes, sir.

Mr. ROGERS. Well, apparently, the definitions were adequate for the IG to feel like that they were not being followed.

Why is it that 7 years have lapsed since this has been updated?

Mr. SAMMON. I would have to get back to you on that. I don't know, sir.

Mr. ROGERS. Okay.

* Documents have been retained in committee files.

Mr. Edwards, did you feel like the definition in the TSA's own policies was adequate for you to discern what were and were not breaches?

Mr. EDWARDS. Thank you, Chairman.

Well, there is no set clear definition, you know. Also even if there is a definition, TSA needs to clearly give guidance on that and TSA needs to follow through.

Mr. ROGERS. So this 10-page directive that TSA has on this does not have a definition that is adequate in your view?

Mr. EDWARDS. I have to get back to you on that, Chairman.

Mr. ROGERS. Well, how did you come up with the number of 58 percent that were reported if you didn't have a definition?

Mr. EDWARDS. We didn't, you know. We came up with the definition.

In my opening statement, I have said, you know, anybody accessing unauthorized area, either through inspections, or getting through, that is clearly a breach, you know.

Mr. ROGERS. It is not rocket science, is it?

Mr. EDWARDS. No, sir.

Mr. ROGERS. Tell me about this hand-written boarding pass.

What did you find? How did that happen?

How does somebody hand-write a boarding pass and get through security? What was the explanation that you found in the records?

Mr. EDWARDS. It was part of our testing, Chairman. I can get back to you on details of that. I don't have it here with me.

Mr. ROGERS. Okay, thank you.

My time has expired.

I recognize the Ranking Member for her opening questions.

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

I see a pathway to fixing what has been laid out by your report, Mr. Edwards.

Are you recommending today that we eliminate TSA and TSO officers?

Mr. EDWARDS. No, ma'am. All we are saying is, based on our audit work, TSA needs to provide clear-cut guidance and have procedures in place, and needs to follow through.

Ms. JACKSON LEE. From your assessment, do you find that a fixable or a doable process? As you look at TSA and TSO officers, do you find that doable?

Mr. EDWARDS. Yes, ma'am.

Ms. JACKSON LEE. Then let me proceed with these questions.

As I ask Mr. Edwards, Mr. Sammon, I am going to be asking you to respond because he said a number of things that I think is extremely important.

Mr. Edwards, explain again about the checking of the application for completeness, and TSA not requiring its TSOs to review the process. Because you are talking about the document that the person who has the right of ingress, of entering the airport, is going to show something, and you are saying TSA is missing-in-action.

Explain that.

Mr. EDWARDS. Well, at the airport when the application is being filled out, in some of the airports we have found there is a quality check process that somebody is looking through the data, and verifying and validating that the data, in fact, is correct.

There is also audits on badging applications to look for common errors. Some airports follow that, but overall it is not being followed.

Also——

Ms. JACKSON LEE. When you say airports, you are talking about not the airport personnel, you are talking about TSA?

Mr. EDWARDS. Airport personnel, you know, they take the information down.

Ms. JACKSON LEE. Right and then——

Mr. EDWARDS. Then it is sent to the Threat Assessment Center——

Ms. JACKSON LEE. Right.

Mr. EDWARDS [continuing]. For them to read it. So there is, you know, inaccurate information that is being entered.

What happens is when TSA's inspectors go to review, the review is not really in detail.

So what we have recommended that when the inspectors go back and review these, make it more detailed inspection and look for these errors. Also recommend look at the quality assurance that some of the airports are following.

Ms. JACKSON LEE. Where do the TSA inspectors intervene? At the point before the application is approved?

Mr. EDWARDS. They routinely come—you know, they do a review of the airports. So when they do that, that is the time they will be looking at that——

Ms. JACKSON LEE. You find that that is a missing element. It is not sufficiently broad-based and TSA doesn't take it sufficiently seriously——

Mr. EDWARDS. Yes, ma'am.

Ms. JACKSON LEE [continuing]. To make sure that it happens.

Mr. Sammon, why not? What are you doing to fix that problem? Your mic is not on, sir.

Mr. SAMMON. In the opening testimony, referred to a rule, a very large and comprehensive rule, called the Universal Fee Rule that has been drafted. It is in the administration's review process.

We agree with the IG's overview of badging processes, that some are good and some are not as good. The airports are responsible for completing the badging, accepting the information, and checking the documentation.

What we want to do is have a much more complete process; require much more stringent enrollment age and training; have the documents submitted through TSA so we can put up front edits for completeness and accuracy; scan the documents in through TSA so we can do this up front. So we are not relying——

Ms. JACKSON LEE. You have to be governed—you said that the rule—what is the potential time frame for that rule being promulgated?

Mr. SAMMON. We would guess that the rule would be—what we are hoping is that it would be out for public comment later this year. It is in executive department review.

Ms. JACKSON LEE. You started working on the rule when?

Mr. SAMMON. Several years ago.

Ms. JACKSON LEE. Okay.

Let me go back to Mr. Edwards again. I think this is enormously important. That is why we are here.

We are talking about breaches and you mentioned that, to Chairman Rogers' question, you know a breach when you see it. A breach is a breach is a breach.

My question is, Mr. Edwards, you are saying there is a failure to keep a detailed and adequate record of breaches that could result in a horrific and terrible incident.

Mr. Edwards, is that——

Mr. EDWARDS. Yes, ma'am.

Ms. JACKSON LEE. So there is no depository where one could go and pull up all of the breaches that have occurred.

Mr. EDWARDS. Well, first, you know, they need to have, you know, like I said earlier and the Chairman alluded to, there needs to be a clear definition of what a breach is.

Then TSA needs to give clear guidance to the airports what to report and when to report. Then TSA needs to follow through with that.

They have the system, PARIS. They need to make sure that the metric, the indicator is there. Also, they can go back and look at the trends and look to see how it is being addressed. That is not there. That is part of——

Ms. JACKSON LEE. So it is setting a standard for airports to adhere to, which we don't have. Therefore that hinders the collection of the data.

Mr. Sammon, why is that not happening?

Why do we not have a complete picture of breaches in America's airports, at least 450 that we are in charge of?

Mr. SAMMON. So we have concurred with the IG's recommendations. The IG, in terms of their report that was issued just recently, they agree that our plan going forward would meet the requirements of that recommendation. But they will keep their recommendations open until we supply them the documentation.

So our people are actively, at this point, putting together the information, the requirements, the system, the training to be able to do that; to have a consistent definition of breaches and reporting and response to breaches across the country.

Ms. JACKSON LEE. Okay, but is that in place now?

Mr. SAMMON. It is being put together right now and being drafted right now, I think.

Ms. JACKSON LEE. I may have an additional question, Mr. Chairman.

I will just yield and just simply say this. Let me put an exclamation point.

I am glad Mr. Edwards said that we need TSA and TSO. That is my commitment continuously.

But he also indicated a wide gap. To hear that the first answer is about a rule and the end of the year, let me put a punctuation mark after now. If not now, when?

I think in terms of security, our functionalities are too slow. It is imperative that we move now.

So I would like to discuss this with you further on an expedited process. I know the rulemaking goes by rules. But clearly we have to put an exclamation mark to moving forward more quickly.

I yield back, Mr. Chairman.

Mr. ROGERS. I thank the gentlelady.

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

Mr. WALBERG. Thank you, Mr. Chairman.

Thank you, Mr. Edwards and Mr. Sammon, for being here.

It is almost, humanly speaking, an impossible responsibility that you all have in screening and making sure that security is 100 percent, because that is really what is has to be.

But even having said that, it is still a requirement that we expect to take place, and hopefully, what we have seen in the report and read will be fodder for continuous improvement.

Mr. Sammon, TSA's Playbook program employs security measures at the direct access points and airport perimeters, as you know, and uses a variety of resources to conduct screening of individuals and vehicles entering the airport operation areas.

Could you provide examples for this committee of the security measures that may be employed at an airport's access point and its perimeter?

Mr. SAMMON. Yes, there may be, in terms of access points and perimeter, particularly for access points, random screening that a team may show up and screen employees, coming through to check badges throughout the airport operations area. There are random challenges for badges to make sure that the people out there are the people who belong there.

You referred to Playbook earlier. We use, if you think of secure flight where we look at watch list passengers who are traveling selectees. We look at patterns.

We may look at particular airports they are going out of, gates. You may have seen random gate screening in terms of EDT and taking swabs of passenger hands. That is risk-driven in terms of intelligence, where we see people traveling, so all these are random elements that take place throughout the airport within the sterile area and the access points and in the airports operations area.

Mr. WALBERG. How often has this program prevented a security breach at airports?

Mr. SAMMON. Again, that particular program has prevented a number. I couldn't give you specific numbers in terms of how many have been prevented.

I think if you look at access control through doors, piggybacking, if people suspect that they may be stopped; if there are TSA people on the other side that it does to a certain extent. It is probably not complete.

A number of airports have various programs in place in terms of technology that prevent piggybacking; camera systems in place that people, operators, can view what is going on at those access control points, but not all airports do.

Mr. WALBERG. Are you required to notify an airport before setting up these additional measures?

Mr. SAMMON. We generally work with the airport law enforcement and security people in terms of what we are doing. We like to include them and have them part of the efforts, because if we can build on their capabilities along with ours, it is a better deterrent and better enforcement than otherwise. Yes.

Mr. WALBERG. According to the report issued by the Department of Homeland Security Inspector General's Office, inspection enforcement analysis tracks and analyzes breach data only upon request, if I understand it correctly, which appears to me to present a potential vulnerability.

Do you agree that this could be a problem?

Mr. SAMMON. Yes, and that is why we concurred with both of the inspector general's recommendations. We are putting plans together that we have shared with the inspector general.

They have concurred that those plans, if properly implemented, would meet their requirements or recommendations.

Mr. WALBERG. Thank you.

Mr. Edwards, has the TSA given you a reason why it tracks and analyzes breach data only upon request, though they have admitted that it is a problem?

Mr. EDWARDS. No, sir.

Even though TSA has agreed to our recommendations, and they are going to implement it, I would, for the record, would like TSA to kind of aggressively pursue and implement our recommendations.

Mr. WALBERG. What does aggressive mean?

Mr. EDWARDS. Well, some of them have taken years just based on the previous question. We wanted TSA—I know it is a challenging monumental task, but we need those recommendations to be implemented.

Mr. WALBERG. Okay.

In the remaining 29 seconds here, Mr. Sammon, while I have the opportunity, and it is on a different subject, Mr. Chairman, forgive me for it, but this is the opportunity.

Anything about the foreign repair stations; is that coming to conclusion here? That is a security issue as well.

Mr. SAMMON. Yes, as we briefed you, and Chairman Rogers, the economic analysis has moved on. It is under executive department review.

So that has moved on in the time frame that we have briefed you on earlier. Yes, sir.

Mr. WALBERG. Well, we are not forgetting that. It is an awful long time it is going on here, and hope to see a conclusion.

Thank you, Mr. Chairman.

Mr. ROGERS. I thank the gentleman.

The Chairman now recognizes the Ranking Member of the full committee, Mr. Thompson, for any questions he may have.

Mr. THOMPSON. Thank you very much.

Mr. Edwards, your testimony before the committee, I want to make sure we are absolutely on the same page.

Presently there is no definition that you could find codified by TSA for a security breach?

Mr. EDWARDS. The definitions are not consistent across all policy, sir, so that is why the definition for our testing, we used the simple definition that I have indicated in my opening statement.

Mr. THOMPSON. So, it is no.

Let me add this. You know, I think we already—I am just trying to get it on the record that is all.

The other point I think we want to make is, Mr. Sammon, what directive in these security breaches did you give TSOs before this IG report came out?

Mr. SAMMON. The TSOs and inspectors throughout the airport are given direction in terms of their screening procedures and processes. We have found that in every case, there have been examples where people have been able to evade or avoid those. So we have continuous training with the officers.

Obviously, the point is to have everyone who is entering the sterile area to have been properly screened. The officers know that, and it is a matter of making sure that the officers and their supervisors are continuously and constantly every day reinforcing it and carrying out the procedures that are required.

Mr. THOMPSON. So your testimony is that rather than a defined statement for what a security breach is, training was the substitute.

Mr. SAMMON. We agree with the inspector general that the less specific definition of a security breach was not helpful. That we need to have a specific definition that everyone understands and uses in implementation across all 450 airports.

Yes, sir.

Mr. THOMPSON. All right.

So what is the latest statistics that you can provide this committee on security breaches that have occurred in airports across the country?

Mr. SAMMON. I would have to provide the committee—be happy to provide those to the committee. But I don't have those specific numbers with me today, sir.

Mr. THOMPSON. Who collects it?

Mr. SAMMON. Our operations department, the Office of Security Operations.

Mr. THOMPSON. So security operation manages the data for security breaches?

Mr. SAMMON. Yes, sir.

Mr. THOMPSON. Is that your understanding, Mr. Edwards?

Mr. EDWARDS. Well, there are so many offices in headquarters in TSA that provides the reporting guidance, and they have the PARIS data system.

But the corrective action on the breaches is taken at the field level. It is not at the headquarters.

Mr. THOMPSON. So, Mr. Sammon, Mr. Edwards just said something different.

Mr. SAMMON. The field-level people he is referring to all report to the Office of Security Operations. All the TSOs, all the inspectors, all the Federal security directors are all under the Office of Security Operations.

Mr. THOMPSON. How is the data for the breaches transferred from the field to headquarters? What is the directive?

Mr. SAMMON. So it would come up through, if there is a breach noted by an employee, they would report it to the supervisor, who would report it to the airport, who then reports it back up in through the system, up to the headquarters, where it is compiled for all 450 airports.

Mr. Edwards, is that your understanding?

Mr. EDWARDS. That is my understanding too, sir.

Mr. THOMPSON. So you agree with that?

Were you able to see any reports of the information transfer at the headquarters?

Mr. EDWARDS. Well, that is where we say there is 42 percent of the reports at the airport and what is reported to headquarters, there is no consistency, because there is no clear guidance on what to report and when to report.

One of our recommendations is that they have to have a comprehensive oversight program where they provide clear guidance on how each of the airports need to be reporting and when, and then TSA needs to follow through.

Mr. THOMPSON. Mr. Sammon, all of us have heard about this incident at the Newark airport.

Was TSA involved in that at all?

Mr. SAMMON. The New York Port Authority had issued the badge for that particular person. He is employed by the New York Port Authority to staff exit lanes at the Newark airport.

So in terms of TSA, he is not employed by TSA. His badging process that the New York Port Authority went through is the process that TSA prescribes.

We have, you know——

Mr. THOMPSON. Describe what that process is.

Mr. SAMMON. In terms of initially, it would be a criminal history records check. It would be a watch list check. It would be immigration status or citizenship status.

Those three things comprise the check.

He had been working there for quite some time. A number of those airports, when we put procedures in, were grandfathered in, in terms of not having to redo criminal history records check or other things.

His identity was run through a criminal history records check and the watch list. It did not show up. He did not hit anything—nor both his assumed identity and his original identity.

Mr. THOMPSON. So your testimony is that there are people working at airports from a security standpoint, who were grandfathered in and we did not do background checks on them?

Mr. SAMMON. They were run with background checks. They were run—the watch list is run on them every single evening.

In terms of their original criminal history records check that was put in when people apply for a badge. They get a criminal history records check.

What we are proposing in this rule, however, is to make the renewal of that criminal history records check every 5 years, the same as it is for all other Federal badging standards.

Mr. THOMPSON. So criminal history does not require identification?

Mr. SAMMON. It requires submission of fingerprints, sir, and identification.

Mr. THOMPSON. So I could—Mr. Chairman, with your indulgence on this.

I am trying to figure out how somebody could put their fingerprint on a badge, and end up having identity of somebody else.

Mr. SAMMON. So he, as I mentioned, the process was he has been in the system for quite some time. He has been working in the New York area under the Airport Authority for quite some time.

He went in—even if you submitted his fingerprints, if he is not a criminal and there is no criminal history, he is not going to make—there is not going to be a match.

So unless either identity, either his real identity or the assumed identity, had a criminal record when you put his fingerprints in, there would be no match in the FBI criminal history records check.

Mr. THOMPSON. So you are saying that there could be a lot of people just like this person in the system because our system is not designed to pick up people like this?

Mr. SAMMON. Again, this is why we want to have this more comprehensive rule. We are using rulemaking because we are making substantial changes to the documentation and verification.

This person apparently has—he assumed an identity. He didn't attempt to do anything other than maintain his job with that identity.

He didn't use it for fraud. There were no criminal nor terrorist associations with——

Mr. THOMPSON. But I think he used it for fraud. He is working under somebody who is dead.

Mr. SAMMON. Right. He was using it for fraud to get that job, yes, sir.

Mr. THOMPSON. Well, I yield back, Mr. Chairman.

Mr. ROGERS. I thank the gentleman.

Listen, I have listened patiently. You all keep making references, both of you, to not having a clear definition as being excuse for these not being reported, and that is just B.S.

The fact is a breach is a breach.

If somebody gets through a checkpoint, a secure access checkpoint, that is not supposed to and it is reported to a supervisor, that ought to be reported up to TSA. I don't care what definition you use.

So please don't excuse that anymore in your remarks. We have got to find a way to make sure every breach, by any definition, is reported up to big TSA and PARIS, so we can come up with processes to fix this.

Chair would now recognize the gentleman from Minnesota, Mr. Cravaack, for any questions he may have.

Mr. CRAVAACK. Thank you, Mr. Chairman, for this very important hearing. I would like to request that we have a field hearing sometime in the future regarding this important issue.

Mr. Sammon, I flew 17 years as an airline pilot. I have got to tell you, if you had asked an airline pilot where—before 9/11—what was going to happen, we would have told you.

I am going to tell you now that I feel the next breach that will occur is going to come from the shadow of the airplane, and coming from the ground, hooking up to a passenger that comes in through clean through the airport.

Would it surprise you, sir, if I told you that several people, both pilots and ground personnel, have told me the security around the aircraft coming from outside sources is a joke?

Mr. SAMMON. I would think that there is a lot of activity on the back side of the airport. There are a lot of different people and crafts coming and going.

The people who have SIDA badges undergo three layers of checks.

Does that prevent all criminal activity and whatever else? It does not.

TSA does random inspections of folks in terms of what they are doing there. We have also had a large number of people on the back side of the airport who have reported activities in terms of contraband being shipped in and out of aircraft.

So, no, it is a very active area, yes, sir.

Mr. CRAVAACK. Okay. I could tell you that I have had people call me up because of my background and telling me—and warning me that this—and I am going to tell you right now, the next incident is going to come from the ground.

It is going to come from the shadow of the aircraft. It is not going to come through the passenger terminal.

I am telling you that. Okay?

Now, I don't know if you are aware, in October 2011 Channel 2 down at Hartsfield-Jackson Airport did an undercover report. This is what they said, the whistleblower that went in: "If I were a crazy lunatic or an Osama bin Laden sympathizer, I can come in and put anything on the plane."

The other comment was, "I can bring a gun in there if I want to, a bomb, anything," said the whistleblower, "that is how easy it is."

So my question to you, sir, is: Do you believe that TSA has sufficient procedures in place to protect the traveling public from an incident from occurring?

Mr. SAMMON. So with regard to the whistleblower, and the story was reported in the Atlanta paper, or the newspaper—or the TV anyway.

First of all, they do not understand the procedures and the law. They don't understand the requirements of what has to be sealed.

In terms of the areas that they are talking about people piggybacking were not a secure area, they are the catering facilities. The allegations in terms of what could or could not be done in terms of what was sealed between the carts and between the trucks, the person does not understand the regulations.

We have also inspected this operation at least 20 times in the past several months and found that in terms of all the regulations, they meet all the requirements that are in place.

Mr. CRAVAACK. Well, it says here—this is part of the thing—it says—he said the carts that were sealed are the liquor carts to keep employees from stealing the liquor. That was really the only things that were consistently sealed.

Mr. SAMMON. So the carts can be unsealed if the truck is sealed or the driver is accompanied to the aircraft. So there is—we have had a running contention with that reporter in terms of his understanding and reporting on what the law says and what the regulation is saying.

Mr. CRAVAACK. Well, we know what the law says and the regulation says. What I am telling you, sir, is that with—this is just a report that has been done.

But I am telling you from people that I know that have been on—that are ground counters around the shadow of the airplane are basically reinforcing what this person is telling me.

So my question—you know, and when asked the TSA responded pretty much what you just said right now, sir.

Now, I am not trying to——

Mr. SAMMON. Right.

Mr. CRAVAACK. This is bigger than pointing fingers. This is about protecting the flying public.

This is ensuring that we don't have another incident like 9/11 ever again. I am trying to fix the problem. I am not trying to point blame, trust me on that.

I am trying to make sure that we never have that incident occur again. We never have an aircraft that is used as a human missile.

So what I am trying to say is pretty much the response to this was all that TSA sent to Channel 2 was a generic statement reiterating that it does regular inspections on airline security operations to make sure everyone is following the rules.

Now with that said, sir, I understand that only 17 percent of the airports have been assessed. Is that correct?

Mr. SAMMON. I think what you are referring to is the JVA.

Mr. CRAVAACK. Correct.

Mr. SAMMON. The JVA is a very in-depth assessment. It is done with TSA and the FBI. It takes quite a bit of time and a limited number of airports are assessed each year.

Mr. CRAVAACK. Okay. Well in all due respect, sir—and I am over my time—we have a very intelligent enemy that very easily can find the weaknesses of a small airport connecting into a larger airport connecting further on.

I don't envy you your job. Trust me when I say that.

But we have to be much smarter than the enemy. I see a lot of holes here.

I am being alerted to a lot of holes. I am telling you where the next incident is going to occur.

So with that, sir, I will yield back.

Mr. ROGERS. I thank the gentleman.

The Chairman now recognizes the gentleman from Louisiana, Mr. Richmond, for any questions he may have.

Mr. RICHMOND. Well, I will just start where my colleague left off, and a very general question.

Mr. Sammon or Mr. Edwards, either one of you can answer it.

But is there a line or protocol or procedure for an employee to call, whether it is a pilot, stewardess, janitor at an airport, so that, when they have these gut feelings about what the next plan may or may not be, that they can report it to somebody so that it is on the radar and you all respond to those reports?

So does something like that exist?

Mr. EDWARDS. Sir, we have a hotline. DHS OIG has a hotline that we get referrals and allegations about a wide variety of issues. We also educate all the DHS employees to refer to when they see a situation like this.

If I may, if I could go back to the Congressman from Minnesota about the concern he had about the shadow of the aircraft.

Sir, that is why we do covert testing. We have done a number in the last several years.

The results of it is classified. I would be glad to come by and brief on the results that we came up with.

Mr. RICHMOND. Mr. Sammon, you also talked about the goal. I think it was having 35 airports in the prescreen program?

Mr. SAMMON. Yes, sir.

Mr. RICHMOND. Where are you up to right now?

Mr. SAMMON. Right now, we are at probably about a dozen or so. Getting up to PreCheck is a function of also adding the additional airlines.

United Airlines will be coming on shortly. U.S. Air will be coming on within the next month or so. Also JetBlue will be coming on later this summer.

So we are getting the airlines up. They are modifying their systems to be able to do this. We expect to be rolling up additional airports over the balance of this year.

Mr. RICHMOND. Also—and I listened to the exchange between you and Ranking Member Thompson about the incident at Newark and what happened and all of that.

What I didn't hear is what procedure could have been in place to prevent it, and is it in place now?

So——

Mr. SAMMON. Again, the types of procedures and process changes we need, in terms of getting data into the system, identifying documents, does require rule-making, unfortunately.

There are impacts on airports. It costs money.

Those procedures that we have outlined, I believe, if we had those in place, it may have caught this gentleman. I can't guarantee it, but it may have.

Mr. RICHMOND. So with the rule-making and things not being done yet, we still don't have a procedure in place to prevent this in the future?

Mr. SAMMON. Right now, the system still has gaps, and that is what this rule-making is intended to address. Yes, sir.

Mr. RICHMOND. I guess the other question just becomes is there a general feedback to TSOs, TSAs, and airport security?

At least in my experience, people try something one time just to see if it works, and they continue to do it. So do we do a continuing education or training or anything to let people know this is the latest attempt in getting into secured areas or getting past certain checkpoints?

Do we do that with our on-the-ground troops?

Mr. SAMMON. Yes, we take—in terms of incidents, not only in terms of the kinds of things that—in terms of access control, but people attempting, testing the system, say shipping cheese with electronics attached to those things, putting those images back for training for TSOs in terms of what to look for and the kinds of things that they should be up to date.

So we have increased the number of TSOs with security background checks so that we can share more intelligence with them. Because we want to keep this feedback not only from where the incident happened but to share it across the country, because they are not isolated. They are generally—things can happen at any location.

Mr. RICHMOND. But in order to do that, the breach has to be reported and put in something so that all of them can be used as teachable moments. Hopefully, we are getting to fewer and fewer teachable moments in the process.

Mr. SAMMON. Yes, we agree, and concur with the IG. Yes, sir.

Mr. RICHMOND. Is there anything else you can do besides something that takes rule-making so that we can prevent people from getting into secured areas, or what happened in Newark, just in case we don't have time to wait on rule-making?

Mr. SAMMON. Our inspection efforts have been increased to working with the IG in terms of things we can do in the near term, in terms of badging process kinds of audits, and information analysis. But also our training at the checkpoint and other areas throughout the airport is being stepped up, because we realize there are process things that have to be done.

But also, in the shorter term, the intensity has to be picked up. Yes, sir.

Mr. RICHMOND. Thank you.

My time has expired. I yield back.

Mr. ROGERS. I thank the gentleman for his questions.

The Chairman now recognizes Mr. Lungren for any questions he may have.

Mr. LUNGREN. Thank you very much. I guess I have got 37 seconds.

So, thank you.

Mr. ROGERS. You have got time.

Mr. LUNGREN. Thank you very much.

Mr. Sammon, first of all, let me just say there is a lot of criticism that has been leveled at DHS and at TSA. It is probably where more Americans get to see—I was going to say are touched by TSA—than any other place in the country.

But we ought to reflect on the successes. I mean, 9/11 was over 10 years ago.

We know the enemy probably wishes to continue to use commercial air traffic as one of the vulnerabilities to attack us. We have been, through a lot of hard work, a lot of people dedicated, and some luck, not subjected to another attack like we were on 9/11.

So I think there are some thanks that ought to be delivered to TSA and those that work.

Having said that, let me ask you about your prescreening expedited passenger program.

Would Henry Kissinger qualify for that?

Mr. SAMMON. I think we saw this morning in *The Wall Street Journal* a very complimentary article from Dr. Kissinger, in terms of how he was treated professionally at the airport. He was—I can pull a copy of the article out——

Mr. LUNGREN. I understand that. But in the mind of a lot of people, it would seem to be a waste of time to subject Mr. Kissinger to extra, sort of——

Mr. SAMMON. Yes, he would qualify if he—again, there are two ways, right now, to qualify: One, through opting in through your airline if you are of a certain level of flying; also through global entry, through CBP.

We are looking at many more ways to say: How do we get trusted people into the system?

I mean, our vision would be that, in the future, the majority of passengers are going through a less physically intensive screening process. Because if we know more about them up-front, that we can improve the level of security while improving the passenger experience through the airport.

Yes, sir.

Mr. LUNGREN. I hope that happens because, frankly, I have heard that with two administrations. I have heard that in classified briefings and in open briefings, that this makes sense, that it would be better for us.

Yet it seems like it is stretched out and stretched out. I am glad that we at least are going forward.

Here is a question I would address to both of you.

This is a serious matter in terms of control points with respect to access. But let us face it. It is a tedious job.

If you are successful, and if most people are not trying to bring something that is prohibited through, you know, 99 percent of the time. I mean, there is a tendency to slack off. There is a tendency to presume that you are not going to find an item that you ought to stop.

So how do you continue to keep the edge?

It would seem to me one of the things is very, very aggressive supervision. I know that part of that is, you know, management versus employees and that sort of thing.

But it just seems to me, that is one of the toughest conundrums that you have.

Mr. SAMMON. Right.

Mr. LUNGREN. I wonder what you would have to say to that.

Mr. Edwards, if, in the reviews that you have undertaken, you have any comment on that?

Mr. SAMMON. So I think your point about supervision is critical. TSA was stood up basically around the country, local hiring, training took place locally.

What we have done is stood up a training program in Glynco, Georgia for the first-line supervisors. Because that is where you make it or break it, in terms of what those supervisors communicate to the employees, what they see, and how they manage those individual checkpoints.

We have not—TSA in its first 10 years had had no central place to run all the supervision through a standardized approach to understanding TSA's mission to TSA's—what we were trying to accomplish at the checkpoint, and maintaining that edge that you are referring to.

So that is—what you brought up is exactly what we have recognized and are beginning to do.

We have run two classes through, the first two classes. I think there is another graduation this week. We are going to be—our goal is to get all the first-line supervisors through that process because that is where you have to begin.

Mr. LUNGREN. Mr. Edwards, is that the proper approach?

Are you satisfied with what they are doing?

Mr. EDWARDS. Yes, sir.

But I also would like to point out, if I may, that, you know, we want to make sure that TSA operates in an optimum fashion. We want to make sure that they bring issues and concerns to you and to the American public to see TSA fix those recommendations in a timely fashion.

I think they add value by bringing—pointing out those issues to TSA. TSA is working towards fixing them, but we would like it to be fixed sooner than later.

Mr. LUNGREN. I would just reflect on this, Mr. Chairman, and that is that in virtually every other endeavor in our society competition has been viewed as one of the ways in which we sharpen our instincts, and sharpen our approaches, and sharpen our performance.

Yet for whatever reason TSA administrators, over the past number of years, have been reluctant to support a program that allows private sector to be involved as an adjunct or a competitor to the regular TSA operation.

I would just say I hope we don't lose sight of that. I know that there are many of us in the Congress that believe that that is one component.

It is not a criticism of TSA employees. But it is one component of how you improve performance. I yield.

Thank you, Mr. Chairman.

Mr. ROGERS. I thank the gentleman.

Before the Chair recognizes Mr. Davis for any questions, the Ranking Member has informed me she needs to leave and wants to make an observation before she has to step out.

The Ranking Member is recognized.

Ms. JACKSON LEE. Thank you, for a moment, Mr. Chairman.

Let me just try to pointedly go back to this question of breaches, which I think really deserves an immediate response. I do want to indicate that I am pleased. I think that the Chairman is having this hearing, and we are joined together at this hearing.

The Members are here, I would say, because of the faith we have in the fine men and women that work for TSA and realizing the work that they do.

I believe Administrator Pistole's concept of a Federal force, if you will, combined with intelligence, information, and fighting counterterrorism is probably the best approach and does not lend itself, from my perspective, though my mind is open, to massive privatization.

The reason I say that are these two pointed questions.

The gentlemen at Newark used identification of a deceased person. We need to get that on the record. He was operating with an identity that could have generated in a heinous incident.

So the question is: Did you do a security threat assessment of what might have happened, Mr. Sammon?

Then with respect to breaches, this also includes airport collaboration. I see a gaping hole while we are sitting here talking to each other about the communication between TSA and airports.

Mr. Edwards, you see the direction that I am going.

Even though you are doing a comprehensive rulemaking at this point, a simple missive, if you will, to your lead officers at these airports, you take the risk assessment approach to indicate that airports are responsible for reporting those breaches.

Why have you not done that simple task, even though the rulemaking is proceeding?

A missive to our 10 most vulnerable, or however the risk assessment is made, Mr. Edwards, would that be a fair approach, even though we are in the middle of rulemaking, to communicate with airports?

Mr. EDWARDS. Yes, ma'am.

Ms. JACKSON LEE. And insist that they provide information of breaches.

Mr. Sammon, can that be done now?

Mr. SAMMON. We can communicate that to our airport operating people and make sure that they do get the breaches reported properly. Yes, ma'am, it can be done.

Ms. JACKSON LEE. I would ask you to do that. I would ask—you cannot answer it now, but I would ask whether or not you have done a security threat assessment of what it meant for a person having a deceased person's documentation for the period of time that this gentleman had it.

I thank the gentleman for yielding.

Mr. ROGERS. I thank the gentlelady.

The Chairman recognizes the gentleman from Illinois, Mr. Davis, for any questions he may have.

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

I trust that the questions I am going to ask have not been already asked. If they have been I apologize for that.

Mr. Edwards, in your testimony you mentioned that you gave six recommendations to TSA in reference to access control vulnerabilities.

Have the recommendations accepted been implemented? If so, what has been the outcome of those recommendations?

Mr. EDWARDS. Out of the—thank you, Congressman.

Out of the six recommendations, TSA has implemented one and has agreed to implement the other five. They are in the process of doing it. They haven't given us detailed information back to us on when they are going to implement the other five.

Mr. DAVIS. I would imagine that there has not been sufficient time to evaluate the impact of the one that is undergoing implementation now?

Mr. EDWARDS. Yes, sir.

Mr. DAVIS. Mr. Sammon, I am actually quoting from your testimony in terms of a statement.

"The Known Crewmember program is the result of a collaborative effort between the airline industry, pilots, and TSA which currently allows uniformed pilots from 20 airlines in 10 airports to show two forms of identification. After evaluation, evaluating operational data from 10 airports, and through much discussion with industry representatives, we are planning to expand the Known Crewmember solution to more airports this calendar year."

Let me ask you, is it a feeling or is it your feeling that there is a one-size-fits-all approach to this? Or is this experimental in a way? Or is it testing an approach?

Could you respond to that?

Mr. SAMMON. I would be happy to.

We had piloted or had tested the approach at about three airports for probably over 2 years. Having had considerable conversations with the various pilot associations and the airline industry, and have come to a rollout approach that we expect to get to over 30 airports by the end of the year.

The pilots are the most trusted person coming through the checkpoint. The pilot does not need an explosive device to damage the plane. So what we want to do is expedite their access.

We actually do more identity verification today through Known Crewmember than is done through the regular process coming through the checkpoint. So we feel that we have a higher identity verification that the person is indeed a pilot. But there is less physical inspection.

Mr. DAVIS. Thank you very much.

Thank you, Mr. Chairman.

Mr. ROGERS. I thank the gentleman.

I will recognize myself for a second series of questions.

Yesterday at this time of the day, I was in New York City at Ground Zero touring that progress there—very sobering. Then to come here today and hear this is just disturbing.

As I told you earlier, regardless of the definition, if a breach was reported by a TSA agent or officer to their supervisor, it should be reported up the food chain, regardless of the definition.

I just can't get past that point.

Mr. Sammon, I have worked with you for a long time and I know you to be an extremely competent fellow who does a lot of things very well. This isn't one of them. I hope that you recognize that this has got to be fixed and fixed quickly.

We don't need a rulemaking. We need your supervisors in the airports to know if a breach is reported to them it goes up—no matter what the definition is—it goes up to PARIS and to you all so you all come up with processes to fix this.

Having said that, when do you think that this definition will be in place? Tomorrow would be a good time.

Mr. SAMMON [continuing]. A good time. People are working on it right now in terms of definition, and we are working on the security operations directives to get them rolled out to the field.

We can get you a timing—I would be happy to get you an update on the timing here.

Mr. ROGERS. I hope you will.

Mr. Edwards, would you agree that given we haven't had the reporting of all breaches, that we really don't know if there is a pattern of breaches that have been occurring for TSA to be able to respond to or prepare for?

Mr. EDWARDS. No, sir. The airports that we looked at and what was reported, we don't have that, sir.

Mr. ROGERS. You don't what?

Mr. EDWARDS. There is—we cannot predict a pattern because it has not been reported up all of them.

Mr. ROGERS. Exactly my point.

Mr. EDWARDS. Yes, sir.

Mr. ROGERS. Until we get 100 percent of these breaches reported, there could be a pattern that is being established by folks feeling their way through these different airports to find out our vulnerabilities. We don't have a way of responding to it.

Mr. EDWARDS. Right. If it is reported back to the PARIS system then they can look at trends and do some analysis to see what the breaches were.

Mr. ROGERS. The Ranking Member wants to ask something right quick.

Mr. THOMPSON. Yes.

Mr. Sammon, you made a statement that a lot of employees at airports were grandfathered.

Do we know how many?

Mr. SAMMON. I don't know off the top of my head. We can get— I would be happy to supply the committee information, but not off the top of my head.

Mr. THOMPSON. I really think the committee really needs that because this is my first time hearing this.

Mr. Edwards, were you aware of this grandfathering?

Mr. EDWARDS. No, sir.

Mr. THOMPSON. Would you be concerned too?

Mr. EDWARDS. Absolutely.

I also would like to point out that even—you know, there has to be—I gave an example in 2007. There has to be periodic and recurrent criminal history checks.

That is one of the findings in our audit. You know, I am definitely concerned just like you.

Mr. THOMPSON. So with 450 airports, and if we grandfathered all these individuals in, Mr. Chairman, we could have any number of people working in airports right now that we don't know whether they are who they say they are——

Mr. ROGERS. That is exactly right.

Mr. THOMPSON [continuing]. Based on the Newark Airport incident.

Mr. Edwards, are you aware of a method that could provide TSA with the identification of the employee and the criminal background that would not require rulemaking to get done?

Mr. EDWARDS. Can I get back to you on that, sir?

We will work on a simple process to get back to you.

Mr. THOMPSON. Well, are you aware of any other agency that is doing—let me just—Mr. Chairman, the general public assumes that every person who goes to an airport that goes through this process is first, who they say they are and whether or not the criminal background.

I am concerned now that we don't have a way of identifying the identity of that person other than some fingerprint that may or may not only show that that person does not have a criminal history but it does not verify identity.

Mr. ROGERS. Right.

Mr. THOMPSON. That is a real concern on my part.

I yield back, Mr. Chairman.

Mr. ROGERS. I thank the gentleman.

I want to go back to something Mr. Edwards said in his opening statement talking about how you found the various employees that had gotten certification badges or access badges at different airports with different information.

Is there not a database where when somebody applies for clearance that they are checked against every other airport?

Is there a single database or clearinghouse for that?

Mr. EDWARDS. Well, there are—the 359 airport offices, badging office that we looked at, we found this anomaly of this one individual having three different birth places.

We brought it to TSA's attention. They immediately fixed—got the correct birth place, and fixed that and completed the—and updated the record——

Mr. ROGERS. That is not my question.

My question is these badges are allowed based on TSA's criteria.

Mr. EDWARDS. Right.

Mr. ROGERS. When an airport is going to grant a badge, do they not have to check it against the database of TSA-approved persons?

Mr. EDWARDS. They have to check the database, but all the fields do not match in order for them to get a valid——

Mr. ROGERS. So the database is worthless then?

Mr. EDWARDS. Right, that is what they tell me.

Mr. ROGERS. Goodness gracious. I don't have any further questions.

Do you have any?

I want to thank the gentlemen for their time. This panel is now dismissed.

We will call up the second panel.

The Chairman now recognizes the second panel.

We are pleased to have several additional witnesses before us today on this important topic. Now, let me remind the witnesses that their entire written statements will appear in the record.

Our first witness, Mr. Mark Crosby, currently serves as chief of public safety and security in Portland International Airport. He will be testifying on behalf of the American Association of Airport Executives.

As Chairman, I recognize Mr. Crosby for his opening statement.

STATEMENT OF MARK CROSBY, CHIEF OF PUBLIC SAFETY AND SECURITY, PORTLAND INTERNATIONAL AIRPORT, TESTIFYING ON BEHALF OF THE AMERICAN ASSOCIATION OF AIRPORT EXECUTIVES

Mr. CROSBY. Thank you, Chairman Rogers, Ranking Member Thompson, Members of the subcommittee. Thank you again for this opportunity to speak before you today on behalf of the American Association of Airport Executives.

As AAAE's security committee chair, and the chief of public safety and security at three airports, including Portland International and three seaports, I can assure you that airport operators take the insider threat to the aviation environment very seriously.

We also take seriously the findings highlighted today by the DHS inspector general. Ten-and-a-half years after 9/11, I still hold monthly conference calls with airport security managers to talk about current issues and to talk about best practices.

It is a very dynamic area of our industry and it continues to evolve.

As you know, TSA is largely responsible for controlling access to sterile areas beyond the security checkpoints. My comments today are focused on the other areas where airports control access via airport-issued security badges.

First, airports are public entities with an imperative to provide the highest levels of security. It is our airport. We work there every day, and we care about it.

In addition to partnering with TSA to meet the core mission of passenger and baggage screening, airports perform a number of inherently local security-related duties, including incident response and managements, perimeter security, employee vetting, credentialing, access control, and local law enforcement functions.

These important duties have long been local responsibilities performed by local authorities in accordance with Federal standards, and subject to Federal oversight.

The public safety professionals that I have the privilege of working with every day to perform these duties at airports are highly trained and have first responder duties that we all value immensely.

While these responsibilities are important, let me focus on badging and access control responsibilities, and urge you to preserve the local role of airports in these areas.

Background check process for airport workers has operated for many years successfully as a partnership between Federal and local officials, with the Federal Government holding the sole responsibility for the security threat assessments; and with local airport authorities operating and managing enrollment, credentialing, badging, criminal history background check adjudication, and access control systems in accordance with strict Federal standards.

Local involvement provides a critical layer of security and gives airports the operational control they require to ensure that qualified employees receive the credentials they need to work in the airport environment.

My final point today is that any effort to increase the Federal role in airport badging in access control procedures will diminish security and divert TSA's attention from its core mission. The underachieving results of the TWIC program in the maritime environment provide my point.

As someone with responsibilities for security in both the airport and seaport environments, I can tell you that any move to shift additional functions in aviation to the Federal Government will diminish security by reducing or eliminating a critical extra layer of security that is already in place at airports.

Pursuing such an approach would scuttle a successful local Federal model that has worked for decades. It would streamline significant efforts already underway at airports to upgrade and biometrically enable the existing airport badging and access control systems, and significantly increase costs to the aviation industry with no demonstrable security benefit.

Members of the subcommittee, the access control systems at airports are unique among other transportation facilities, and have operated successfully for decades.

That is not to say there isn't areas for improvement. As was mentioned earlier, the threat is always changing, therefore our measures need to change and improve as well.

Local involvement provides a crucial additional security layer that should not be discarded. That concludes my comments.

I look forward to your questions.

[The statement of Mr. Crosby follows:]

PREPARED STATEMENT OF MARK CROSBY

MAY 16, 2012

Chairman Rogers, Ranking Member Jackson Lee, and Members of the subcommittee, thank you for the opportunity to be with you today to discuss airport access control—an important security function that local airport operators have held for decades in accordance with strict Federal standards, requirements, and oversight. I am testifying today on behalf of the American Association of Airport Executives, which represents thousands of men and women across the country who manage and operate the Nation's airports. I am actively involved with AAAE as chair of the association's Transportation Security Services Committee.

In addition to my work with AAAE, I currently serve as chief of public safety and security for the Port of Portland in Oregon, a joint port authority that operates three seaport terminals and three airports, including Portland International Airport (PDX). In that capacity, I have overall responsibility for Emergency Management at the Port and manage the Port's Public Safety and Security Department, which includes the Airport and Marine Security Departments, the Airport Police Department, Fire Department, and the Communications Center. I have also served on the Public Safety & Security Steering Group for Airports Council International—North America. I am a graduate of the U.S. Air Force Academy and serve currently as a colonel in the Oregon Air National Guard.

Mr. Chairman, I want to assure you and the Members of the subcommittee that airports take recent incidents and the prospect of the "inside threat" in the aviation environment seriously. Airport executives are working constantly in collaboration with the Transportation Security Administration to enhance the layers of security that exist to identify and address potential threats in the airport environment, including extensive background checks for aviation workers, random physical screening of workers at airports, surveillance, law enforcement patrols, robust security training, and the institution of challenge procedures among airport workers, to mention a few. In the public areas of airports, local law enforcement presence and patrols provide security far beyond what is typically in operation at other potential public targets such as sport stadiums, train stations, or shopping malls.

The title of today's hearing poses the question as to whether recent incidents are an anomaly or the sign of systematic failure in terms of access control at airports. From my perspective and the perspective of AAAE, the existing access control system at the Nation's airports works well and is continuously improving. It relies on local management of credentialing and access control systems in accordance with strict Federal standards, requirements, and oversight; a robust, multi-layered security apparatus; and extensive efforts to identify "bad" people before they are ever given access to security sensitive areas of airports. That is not to say that the current system is infallible or that improvements cannot be made. Airport executives, for example, are aggressively working to enable voluntary migration to biometric-based badging and access control systems at airports as part of an initiative known as the Biometric Airport Security Identification Consortium. Other efforts to enhance airport access control technology and procedures are underway as well.

In our view, the best approach to enhancing access control at the Nation's airports lies with continuing to focus on robust background checks, maintaining our multi-layered security approach, and preserving and protecting the critical local layer of security that airports provide with credentialing, access control, and other inherently local functions. While some have argued for Federalizing virtually all security responsibilities in airports, doing so would add to TSA's already daunting mission and abandon the successful local systems and process in place that have proven effective for decades in enhancing security and ensuring efficient airport operations. From a security and resource perspective, it is critical that inherently local security functions remain local with Federal oversight and backed by Federal resources when appropriate.

AIRPORTS ADD A CRITICAL, LOCAL LAYER OF SECURITY THAT MUST BE PRESERVED AND PROTECTED

As you know, airports play a unique and critical role in aviation security, serving as an important partner to the TSA in helping the agency meet its core mission of passenger and baggage screening. The significant changes that have taken place in airports over the past decade with the creation of the TSA and its assumption of all screening duties have been aided dramatically by the work of the airport community, and we will continue to serve as a critical local partner to the agency as it continually modifies its operations with PreCheck and other risk-based approaches to security, which we fully support.

In addition to partnering with TSA to meet its core mission, airports as public entities provide a critical local layer of security, performing a number of inherently local security-related functions at their facilities, including incident response and management, perimeter security, employee vetting and credentialing, access control, infrastructure and operations planning, and local law enforcement functions. These important duties have long been local responsibilities that have been performed by local authorities in accordance with Federal standards and subject to Federal oversight.

Airport operators meet their security-related obligations with a sharp focus on the need to protect public safety, which remains one of their fundamental missions. The professionals who perform these duties at airports are highly trained and have the first responder duties that I know each and every Member of this subcommittee, the Congress, and the country value immensely.

PRESERVING THE LOCAL ROLE OF AIRPORTS WITH BADGING AND ACCESS CONTROL IS CRITICAL

A cornerstone of security within the Nation's airports is the credentialing and background check processes that all workers must undergo prior to receiving airport-issued credentials that grant access to security sensitive airport areas. While a relatively new concept in the maritime environment, credentialing tied to strict, Federally-specified access control has been a key component of security at airports for more than 20 years. I have included a 1-page document at the end of my testimony that provides additional details on airport badging processes and requirements.

In the aviation environment, the background check process for workers operates successfully as a Federal/local partnership with the Federal Government holding sole responsibility for criminal history record checks, security threat assessments, and other necessary Government checks for prospective workers and with local airport authorities operating and managing enrollment, credentialing, badging, criminal history background check adjudication, and access control systems in accordance with strict Federal standards.

The current system for aviation ensures the highest level of security by combining the unique local experience, expertise, and knowledge that exists at individual airports regarding facilities and personnel with Federal standardization, Federal oversight, and Federal vetting assets. Local involvement provides a critical layer of security and gives airports the operational control they require to ensure that qualified employees receive the credentials they need to work in the airport environment.

In contrast to the long-standing locally-controlled credentialing and access control apparatus that exists in the aviation environment, the credentialing/access control system in place in the maritime environment with the Transportation Worker Identification Credential (TWIC) program is relatively new. Under the TWIC model, the Federal Government or its contractors are responsible for virtually all aspects of credentialing, including worker enrollment, applicant vetting, and credential issuance.

Some have suggested abandoning the successful local systems and processes already in place at airports with badging and access control to expand TSA and the Federal Government's control over more of the process as is the case with TWIC in the maritime environment. Airport executives oppose any move to shift any additional functions in aviation to the Federal Government and believe that such a move would diminish security by reducing or eliminating a critical, extra layer of security that is already in place in airports.

Pursuing such an approach would scuttle a successful local/Federal model that has worked well for decades, eliminate local operational control, stymie significant efforts already underway at airports across the country to upgrade and biometrically enable existing airport badging and access control systems, and significantly increase costs to the aviation industry with no demonstrable security benefit.

While the desire to centralize and Federalize the process for all transportation worker vetting programs may be understandable from the Federal Government's perspective, airport executives are concerned about Federal intrusion into existing processes that have worked well for decades. Airports are also very concerned about having to help foot the bill for these initiatives—estimated at $633 million through 2025 in appropriations and new fees as part of the TTAC Infrastructure Modernization (TIM) program—for changes that provide them with no demonstrable security or operational benefit. The current system in aviation operates efficiently and effectively at a fraction of the cost of other transportation vetting programs and at no cost to the Federal Government. Airport executives want to ensure that remains the case.

With the Federal Government and State and local governments operating under historic budget constraints, it makes little sense to devote hundreds of millions of dollars in scarce resources to Federalize functions that airports have performed successfully for nearly a decade. The TIM effort fails to take into account the long-proven approach that exists in the aviation industry.

BIOMETRIC AIRPORT SECURITY IDENTIFICATION CONSORTIUM (BASIC)

Before concluding, I want to take this opportunity to bring the subcommittee up to date on a related topic and the efforts of the Biometric Airport Security Identification Consortium or BASIC initiative. In simple terms, the objective of BASIC is to define a comprehensive, airport-driven Concept of Operations that will enable voluntary migration to biometric-based badging and access control systems at airports—a goal that I know subcommittee Members share. More than 40 airports of all sizes actively participate in BASIC. I would note that BASIC airport participants are working cooperatively with TSA on this initiative as well as with other groups, including the Airport Consultants Council.

Many airport operators—including the Port of Portland—are eager to move forward with biometrics, but concerns remain about the prospect of overly prescriptive and costly solutions. Airports are also eager to avoid repeating mistakes made in the past where the Federal Government required costly and often proprietary access control systems to be deployed in airports in a compressed period of time. That approach proved both expensive and ineffective.

In an effort to avoid unnecessary regulations and a one-size-fits-all mandate regarding biometric-based systems, airports participating in BASIC have identified several key principles that must be part of any future biometric-based badging and access control systems, including:

- Safeguards on local control and issuance of credentials,
- Leveraging of existing capital investments and resources,
- Standards-based open architecture and local determination of qualified vendors, and
- Phased implementation that migrates over time.

In addition to building on the processes and regulations already in place at airports today, BASIC is also working to adapt important Federal standards regarding secure biometric credentials into the airport's operational environment. For example, Federal Information Processing Standard (FIPS) 201 and the more recent Personal Identity Verification Interoperability (PIV–I) for Non-Federal Issuers are reflected throughout the BASIC Concept of Operations and greatly inform the recommended phased implementation for airports.

The BASIC working group, which meets on a regular basis, is moving forward aggressively to update and refine a detailed Concept of Operations that will define the biometric components and common business processes that need to be added to airports' existing procedures to enable biometric-based badge and access control systems in a reasonable and cost-effective time frame. In fact, several airports have already begun to implement the early phases of the BASIC Concept of Operations. Newark Liberty International Airport, San Francisco International Airport, Aspen Pitkin County International Airport, Los Angeles International, and Salt Lake City International Airport—to name just a few—have implemented a secure messaging structure for the submission of biographic security threat assessments and biometric criminal history record checks that will ultimately enable the return of trusted biometrics back to the airport for use on credentials or in access control systems.

Airports are committed to moving forward to bring biometrics into the airport environment as soon as possible in a manner that builds upon existing capabilities and limits operational difficulties. The BASIC initiative, which is being driven by airports in cooperation with the Federal Government, offers the best opportunity for making the promises of biometrics a reality in a timely manner.

Mr. Chairman, in closing, let me thank you once again for the opportunity to testify today. As an experienced security professional responsible for managing public safety and security operations at airports as well as vibrant maritime port facilities in my home of Portland, I am proud of the important role that local officials play in ensuring the highest levels of security and safety within critical transportation facilities.

As I have highlighted throughout my testimony, the access control apparatus at airports is unique among other transportation facilities and has operated successfully for decades. Airport operators, which are extensions of local government, are directly responsible for credentialing and access control under strict Federal rules and oversight in recognition of the security and operational expertise that exists at the local level. Local involvement provides a crucial, additional security layer that should not be discarded.

The current system in aviation leverages local experience, knowledge, and expertise with Federal standardization and vetting assets. Airport operators know and understand their facilities, and they maintain decades-old relationships with the numerous parties that employee individuals throughout the airport environment, resulting in high levels of security.

Abandoning a decades-long record of local expertise and investment in favor of an unproven system under which credentialing and access control would be controlled centrally out of Washington or elsewhere—as is being attempted in the maritime environment with TWIC—would be a huge step backwards in terms of security from where we are now with aviation.

We appreciate your leadership and the work of this subcommittee to preserve and protect the important role that local airport officials play in partnership with TSA to ensure the highest levels of security at their facilities.

I look forward to answering any questions you might have.

ATTACHMENT.—AIRPORT BADGING REQUIREMENTS AND PROCESSES

HISTORICAL CONTEXT

Airport operators and the aviation industry have a robust history of credentialing and access control experience. Since the inception of this approach more than 20 years ago, airport operators have been delegated badging authority by the Federal Government. In the early 1990's airports installed access control systems that for the first time were tied to a credential. In 1996, airports started utilizing criminal history record checks (CHRC) conducted by the FBI to adjudicate employees whose employment backgrounds could not be verified.

CURRENT REQUIREMENTS AND PRACTICES

Since shortly after the September 11, 2001 terrorist attacks, CHRCs have been conducted on all employees with access to the Secure Identification Display Areas (SIDA) and Sterile Areas. Beginning in October 2007, TSA regulations also require name-based security threat assessments (STAs) for all individuals applying for either a SIDA or Sterile Area badge.

The FBI performs CHRCs and provides airports with the full results of an applicant's check. TSA performs STAs, which check an individual against the Terrorist Screening Database and "determines whether there are any outstanding immigration, terrorist or federal open wants or warrants issues pending against the potential employee." TSA provides airports with either "approved" or "disapproved" status for a prospective employee only based on security sensitivities.

Airport operators maintain responsibility for worker enrollment, and badging, issuing local badges with card topography and identifying features unique to that airport facility. By regulation, airport operators and air carriers are responsible for adjudication of the CHRC which allows airport operators to know more about individuals that have access to their facilities. In some cases an individual is not disqualified under CHRC rules; however the individual may require further scrutiny or at least situational awareness for the Airport Security Coordinator. This approach provides a critical local layer of security.

FEDERAL/LOCAL PARTNERSHIP IN AVIATION—UNIQUE AMONG OTHER TRANSPORTATION MODES

In the aviation environment, the background check process for workers operates successfully as a Federal/local partnership with the Federal Government holding sole responsibility for STAs and other necessary Government checks for prospective workers and with local airport authorities operating and managing enrollment, credentialing, badging, criminal history background check adjudication, and access control systems in accordance with strict Federal standards.

The current system for aviation ensures the highest level of security by combining the unique local experience, expertise, and knowledge that exists at individual airports regarding facilities and personnel with Federal standardization, Federal oversight, and Federal vetting assets. Local involvement provides a critical layer of security and gives airports the operational control they require to ensure that qualified employees receive the credentials they need to work in the airport environment.

Mr. ROGERS. I thank the gentleman.

The Chairman now recognizes my colleague from Minnesota who will introduce our next guest.

Mr. CRAVAACK. Thank you Mr. Chairman.

I would like to introduce Captain Sean Cassidy. Captain Cassidy serves for Alaska Airlines, and ALPA's first vice president.

Captain Cassidy has served as both chairman and vice chairman of Alaska Airlines Master Executive Council, and he was the chairman of Alaska Air Group Labor Coalition from 1999 to 2009.

Hired by Alaska in 1996, Captain Cassidy serves as a Boeing 737 captain, has thousands of hours in the air.

Most importantly, prior to his airline experience, Captain Cassidy serves as an officer in the United States Navy as a pilot.

Captain Cassidy has performed duties in the carrier-based EA–6B which is the hardest aircraft to bring on the aircraft carrier, and supported numerous military operations including those in the Persian Gulf, and finished his naval career flying the C–9 as an officer in the United States Naval Reserves.

With that, I would like to welcome Captain Cassidy.

I will yield back to the Chairman.

Mr. ROGERS. I thank the gentlemen.

Captain, you are recognized for your opening testimony.

STATEMENT OF SEAN P. CASSIDY, FIRST VICE PRESIDENT, AIR LINE PILOTS ASSOCIATION, INTERNATIONAL

Mr. CASSIDY. Thank you, sir. On a side note, my wife was an Air Force pilot. I think she might beg to differ with you, sir.

So good morning, Mr. Chairman, Ranking Member Thompson, and Members of the subcommittee, as the introduction said, I am Captain Sean Cassidy, the first vice president of Airline Pilots Association International. I represent 53,000 pilots, both in the United States and Canada at 37 different airlines.

Controlling access to secure airport areas is critically important to the safety and security of the airline industry and the traveling public as we have certainly demonstrated today. While the Transportation Security Administration and airport authorities do a good job of controlling and preventing unauthorized access to these areas, it is my hope that both the TSA and the individual airports involved will continue to develop better response strategies.

ALPA believes that like the vast majority of airline passengers, the overwhelming share of airline workers are trustworthy individuals who want to see their airlines and their industry succeed.

In this context, the insider threat to passenger and all-cargo airline operations has always existed. Advances have been made in identifying those individuals who are reliable versus those who could pose a potential threat.

However, effort is still needed to enhance the security of airlines and airports by ensuring those who have access to aircraft and payloads are appropriate to do so.

The solution lies in advancing a risk-based approach to aviation security, and achieving one level of security for all airline operations regardless of whether they fly passengers or cargo.

Unfortunately, a significant disparity exists today between the security of passenger and all-cargo flight operations. This gap is a serious concern for ALPA.

For example, the Air Cargo Final Rule of 2006 does not require all airports that serve all-cargo airline operations to establish security identification display areas, otherwise known as SIDAs.

As a result, the individual with access to secured areas of the airport are background-checked only through a biographic process, rather than through fingerprint-based criminal record history checks that are required for airline employees working similar jobs at passenger airlines.

The U.S. Government has publicly acknowledged that a fingerprint-based system provides greater security, and a long-established precedent exists for using these systems. Moreover without such a system, we cannot reliably determine whether a person has been convicted of any of the 28 prohibited crimes that preclude access to secure airport areas.

Just as practical experience has shown that the vast majority of airlines passengers have no harmful intent, the same can be said for aviation workers.

We need to do more to identify those prospective employees who pose no threat, so that greater resources can be focused in identifying those who may pose a threat.

One example of the kind of risk-based security that is needed is the ALPA- and Airlines for America-sponsored enhanced crew screening system for pilots known as Known Crewmember. This Government-approved alternative means of access to sterile areas of airports is available to pilots who comply with Known Crewmember requirements.

Known Crewmember has been implemented at seven airports, and 11 more are expected to receive the system soon. ALPA and A4A have encouraged the TSA to include flight attendants in this program.

The Known Crewmember program is just one example of risk-based security. By properly vetting, training, harnessing, and empowering airline workers much more can and must be done to employ them as part of the solution to advancing overall aviation security.

Adopting a threat-based approach must also mean creating and fostering a security culture at airlines and airports in the same way that our industry has sought to achieve a safety culture.

Such a security culture needs investments from airline, airports, and regulatory leaders, and decisive action to establish and enforce a true security culture. Achieving a security culture will call for these organizations to place more emphasis on providing meaningful, practical security training for all employees.

A security culture will also require that all airline airport workers become the eyes and the ears for potential threats.

With me today is airline—pardon me, Alaska Airlines First Officer Ed Finnegan sitting right behind me in the red tie, who I am pleased to say was concerned enough about this issue to take the time to contact his congressman, Congressman Cravaack. Also he is here with us today.

He is a great example of how professional airline pilots stand ready to help advance aviation security in every way possible.

One hundred percent screening of individuals entering the secure areas of airports is not the answer to counter the insider threat. Rather, we need to develop and immediately implement a risk-based systematic method of employee vetting that includes fingerprint-based criminal history background checks of every employee with unescorted access to passenger and cargo aircraft in our operations areas.

To this end, Congress must take action to ensure that full SIDA requirements are mandated for all airports serving Part 121 all-cargo operations.

A risk-based approach to aviation security, coupled with more traditional methodologies and a commitment to building a security culture at all airlines and airports, will help our industry reduce the insider threat at a very reasonable cost.

Equally important, realizing such an approach will enhance aviation security for all who depend on air transportation. It will ensure the U.S. airline industry continues to fuel the Nation's economy.

Thank you.

[The statement of Mr. Cassidy follows:]

Prepared Statement of Sean P. Cassidy

May 16, 2012

Mr. Chairman and Ranking Member Jackson Lee, thank you for the opportunity to testify. The Air Line Pilots Association, International (ALPA), representing more than 53,000 pilots flying for 37 airlines in the United States and Canada, is the world's largest professional pilot association and the world's largest non-Governmental aviation safety organization. We are the representative for the majority of professional airline pilots in the United States with a history of safety and security advocacy spanning more than 80 years. As the sole U.S. member of the International Federation of Airline Pilots Associations (IFALPA), ALPA has the unique ability to provide active airline pilot expertise to aviation safety and security issues worldwide, and to incorporate an international dimension to safety and security advocacy.

OVERVIEW

We applaud the subcommittee's demonstrated interest in airline and airport security by holding this hearing on airport access and other, related subjects.

Maintaining and enforcing effective control of access to sterile and secure airport areas is critically important to the safety and security of the airline industry and the traveling public. The Transportation Security Administration (TSA) reviews and approves mandated Airport Security Programs (ASPs) which must be followed by our Nation's certificated, commercial airports.

ASPs must delineate effective measures designed to preclude unauthorized access to sterile and secure areas, and also must provide effective response protocols in those instances where unauthorized access is attempted or occurs.

To comply with these mandated security measures, airports utilize a variety of mechanisms, to include: Security Identification Display Area (SIDA) protocols; security training and challenge protocols for SIDA badge-holders; perimeter fencing and physical barriers; sophisticated technologies to prevent and detect unauthorized entry into sterile and secure areas; law enforcement patrol and response; and, interior access control systems which incorporate both technological and human resources.

Airport screening checkpoints play a prominent role in an airport's security plan, providing access and screening controls to airport sterile areas for passengers, aviation and airport workers. Airports work in close partnership with the TSA to facilitate the checkpoint screening process.

Accompanying these required airport access control measures dictated in the ASP are certain other TSA policy mandates, normally implemented through Security Directives (SDs) or Emergency Amendments (EAs), which obligate airports and aviation workers to enforce and follow prescribed protocols related to accessing sterile and secure airport areas, and, at times, dictating specific protocols aviation workers must follow as pertains to traditional checkpoint screening, or, alternative forms of approved screening prior to entering sterile and secure airport areas.

The ALPA- and Airlines for America-sponsored security screening system for pilots, Known Crewmember (KCM), is an example of a Government-approved, alternative means of access to sterile areas of airports which is available to pilots who comply with KCM requirements. KCM has been implemented at 7 airports thus far, with 11 more that have been identified to receive the system soon and many more thereafter. ALPA and A4A have encouraged the TSA to include flight attendants in this program, as they should be part of risk-based security.

It has been ALPA's general experience that TSA and airport authorities do a very good job in controlling and preventing unauthorized access to sterile and secure airport areas. There have been some documented failures in this regard, causing inconvenience to passengers and resulting in a negative impact on the timeliness of airline and airport operations. However, we know of no such instances which involved persons who possessed the intent to do harm to the aviation industry. Based on the specifics of these reported incidents, we believe that both TSA and airports have developed sound strategies intended to prevent their reoccurrence.

It has also been ALPA's experience that, in general, aviation workers comply with Government requirements regarding entry into airport sterile and secure areas. Because of practical constraints or operational needs, those regulations do not require all such workers to undergo traditional checkpoint screening protocols prior to entry, but apply alternative means of screening instead. It is normally in this context that discussion ensues regarding the "insider threat" to aviation.

SOURCE OF THE THREAT

The insider threat to passenger and all-cargo aviation operations has always existed in aviation security; it is not a new threat. It is one that must always be addressed, so that the risk of this threat causing a serious event is minimized to the maximum, practical extent. Notwithstanding the advances that have been made in passenger and cargo screening since 9/11, and the reliability of most aviation employees, a concentrated effort is needed to identify and eliminate threats posed by individuals who have access to commercial aircraft and their payloads.

Shortly after the Christmas day 2009 underwear bomber's thwarted attack on NWA Flight No. 253 as it approached Detroit, ALPA published a white paper entitled *Meeting Today's Aviation Security Needs: A Call to Action for a Trust-Based Security System.* In it, we cited the need for a more comprehensive, threat-based approach to aviation security, stating: "The insider threat to the aviation industry must not be overlooked or minimized. It must be addressed along with enhanced screening capabilities; background checks should be conducted on all those with access to our airplanes."

Historically, the insider threat has been well-documented, both internationally and domestically. Al-Qaeda in the Arabian Peninsula (AQAP) has attempted to facilitate the hiring of flight attendants, baggage handlers, and airport security personnel, and in 2010, a Taliban sympathizer gained employment as a baggage handler at a U.S. carrier and traveled to Afghanistan to provide assistance in fighting against U.S. forces.

While we believe that the vast majority of individuals employed by the airlines and Government agencies at the airport are upright, responsible, and trustworthy, no organization is immune from the possibility of employing individuals who engage in criminal behavior. Criminal organizations in the United States have regularly used airport, airline, Government, and contract employees to facilitate criminal activities in the airport environment, which include, but are not limited to, drug trafficking, contraband smuggling, theft, and prostitution. In March, a security officer in Buffalo, NY was criminally charged with allowing passengers to pass through screening checkpoints while using false identification, and as recently as last month, Federal drug agents arrested two former and two current security personnel at Los Angeles International Airport on drug trafficking and bribery charges.

Fortunately for the traveling public, the insider threat has primarily been associated with the perpetration of criminal rather than terrorist activity. However, just as a criminal organization can infiltrate a segment of the aviation work force or circumvent existing security procedures, so too can a terrorist organization. Whether breached by a willing participant who is working for a criminal or terrorist organization, or an unwitting dupe believing he is simply facilitating a criminal rather than a terrorist act, existing weaknesses which facilitate these dynamics must be identified and corrected.

Vulnerability and risk associated with the insider threat is magnified because risk-based security measures have not yet been applied to the extent that they are needed. One example: The May 2006 Air Cargo Final Rule did not require all airports which serve all-cargo airline operations to establish Security Identification Display Areas (or SIDAs). Many persons with access to air operations areas of these airports and to wide-body cargo aircraft are background-vetted only by means of a biographic-based Security Threat Assessment (STA) process, rather than by means of a fingerprint-based Criminal History Records Check (CHRC) which is required for similar employee categories in the passenger airline domain.

This lack of standardized application of fingerprint-based CHRCs in background-vetting of aviation workers exists even though the Government has publicly acknowledged that a fingerprint-based CHRC provides a greater degree of security than an STA, and that there should be congruency in background vetting for workers in functions that present similar security concerns, such as checked baggage screeners and cargo screeners. As a result of this imbalance in background-vetting standards, many persons holding positions of trust in the all-cargo domain, and who have unescorted access to cargo aircraft, the goods they carry and to air operations areas of airports, are not vetted to the same standard as persons occupying equivalent positions in the passenger aviation domain.

There is long-established precedent for using fingerprint-based CHRCs in determining an individual's suitability for hiring in a security-sensitive position. Numerous employment categories exclude convicted felons from eligibility, deeming them to be unsuitable candidates due to security concerns, character issues, and recidivism rates. The difference between undergoing CHRC-based background vetting as opposed to a STA is significant when viewed in terms of the dangers presented by the insider threat. Without use of a fingerprint-based CHRC, no reliable determination can be made as to whether a person has been convicted of any of the 28 prohibited crimes that are described in 49 CFR § 1544.229, and which preclude unescorted access to secure airport areas. This lack of standardization between the background-vetting processes applied to workers employed by passenger airlines and all-cargo carriers unnecessarily creates yet another challenge in mitigating the insider threat to aviation.

REASONABLE EXPECTATIONS

To effectively mitigate the problem of the insider threat to aviation, we must begin with reasonable expectations, have a good understanding of the industry's operational environment, acknowledge that there can never be total elimination of risk and accept the fact that the best we can hope to achieve is reasonable mitigation of the threats we face. It is also necessary to recognize that a certain degree of trust must always exist within the framework of securing the aviation domain. For the system to work, we have to trust Federal Security Directors, Transportation Security Officers, airport law enforcement officers, air traffic controllers, pilots, flight attendants, aircraft mechanics, et al. If we did not, the industry would be paralyzed.

History has demonstrated that "trust" is a very fluid dynamic which offers no guarantees. Aldrich Ames and Robert Hanssen attained the highest levels of trust within their respective agencies, but ultimately compromised the values they had sworn to protect and the security of their Nation. Fortunately, such events are extremely rare and despite the uncertainties which will always accompany the allocation of "trust," so doing is a necessary component of any security system. It is in this context that the concept of "trust, but verify" takes on significance.

RECOMMENDATIONS FOR MITIGATION

Since its creation following the 9/11 attacks, the TSA has continued to evolve its passenger screening measures in an attempt to address the challenges posed by an intelligent, adaptive terrorist adversary. We have witnessed the evolution of Advanced Imaging Technology and the increased use of Behavioral Detection Officers.

Regardless of the tremendous advances in airport screening capabilities, however, we only have to recall the incident of the infamous "underwear bomber," or last week's reports that intelligence and law enforcement agencies had identified and interdicted an IED created entirely of non-metallic material reportedly designed by an AQAP master bomb-maker to be detonated by a suicide bomber aboard an aircraft.

Although technology plays an integral role in the aviation security process, it is not a stand-alone solution. TSA Administrator John Pistole has recognized this fact by applying a more risk-based, threat-driven approach to aviation security, as evidenced by his support of the Known Crewmember program and other special screening programs such as Global Entry, Pre-Check, I-Step, SPOT, and behavioral detection techniques. The DHS public message of "If you see something, say something" is a valuable public awareness campaign to help mitigate the threat of terrorism.

HARNESSING EXISTING RESOURCES

Aviation workers, which number in the hundreds of thousands, represent a vast and under-utilized resource in protecting the aviation domain, to include combating the insider threat. Commercial pilots, all of whom have undergone security awareness training as part of their employment, know their segment of the aviation industry and can sense anomalies whether commuting for work, on personal travel, or flying their assigned routes. Just as a police officer knows the beat he patrols and the mailman knows the neighborhood in which he delivers, so does the pilot know his or her normal work environment. As such, pilots should be considered assets in identifying threats to the industry, including insider threats, and treated as part of the solution rather than being viewed as part of the problem. This logic can be applied to other classes of aviation workers who frequent the airport domain: Flight attendants, mechanics, caterers, fuelers, baggage handlers, airport service providers, et al.

In the late 1990's, ALPA served on the Government/industry Employee Utilization Working Group (EUWG) for the purpose of identifying guidelines to be followed by aviation sector employees to enhance security. One of the recommendations ALPA made to that group was to focus on the largely untapped resource of airport, airline, and other tenant employees. All of the individuals who work at an airport, regardless of position, background, and experience, and can usefully serve as the "eyes and ears" of security.

Regrettably, the EUWG's recommendations have been largely ignored, but we believe that this hearing provides an opportune time to revisit them, because they are still valid:

- Encourage and assist airports and air carriers to develop and implement security awareness programs which emphasize the "team" concept.
- Encourage each airport and airline to employ or designate an existing employee as a security training manager.
- Create a standing security awareness working group comprised of Government and industry representatives for the specific purpose of enhancing employee's security awareness and compliance.
- Perform human factors research into why security lapses occur, applying lessons learned from that research to future employee awareness training efforts.
- Encourage certain employee groups (e.g., baggage handlers) to have their members serve as candidates to be used as a security observer/auditor for a few hours each month on a rotating basis when schedules allow. Employees should be utilized in this fashion in order to make them more security-conscious.
- Create a common, easily remembered, and dedicated phone number for specific employee use at airports for reporting of suspicious behavior or security breaches.
- Maintain a repository of employee utilization and security awareness media, including videos.

Just as practical experience has shown that the vast majority of airline passengers have no evil intent and represent no threat to aviation, the same can be said for the vast majority of aviation workers. By properly vetting, training, harnessing, and empowering them, much can be done to counter the insider threat.

The accomplishment of this goal will require a paradigm shift within the aviation domain. Just as the airline industry has placed great emphasis on the use of Safety Management Systems (SMS) in order to achieve and maintain aviation's excellent safety record, similar emphasis must be placed on the development and maintenance of a comprehensive security management system.

The successful completion of this task will require true buy-in from the leadership of critical aviation stakeholders such as airlines, airports, and regulators, and their definitive action in the establishment and enforcement of a true security culture within their respective organizations. It will require these entities to invest more resources in and place more emphasis on providing meaningful, practical security training to employees and their empowerment as valued security resources, rather than simply "checking the box" in meeting Government mandates regarding the length and content of security training. Only in this way can a true security culture be established.

CONCLUSIONS

One hundred percent physical screening of individuals entering secure/sterile areas of airports is not the answer to the insider threat. A highly-developed, systematic and reliable method of employee vetting, including fingerprint-based criminal history background checks (CHRC) of every employee with unescorted access to passenger and cargo aircraft, air operations areas, baggage and cargo should be implemented to support a risk-based approach to identify "evil intent." To this end, full SIDA requirements must be mandated for all airports serving FAR part 121 all-cargo operations. In addition, fingerprint-based CHRCs must accompany the STA process in the background vetting of all individuals who have unescorted access to all-cargo air operations areas, aircraft, and the cargo they carry.

If the leadership of critical aviation stakeholder organizations and regulators commit themselves to following through on the aforementioned recommendations, and if aviation workers are properly vetted, provided the appropriate training and reporting mechanisms and then empowered, they can be counted upon to counter the insider threat.

This approach to aviation security, coupled with other more traditional methodologies such as the use of random inspections, employment of technological assets, such as surveillance and detection equipment, will do much to mitigate the insider threat, at very reasonable cost.

ALPA is grateful for the opportunity to be heard on this important matter and to provide its views to the subcommittee.

Mr. ROGERS. Thank you, Captain Cassidy, for your testimony.

Our third witness, Mr. William Swift currently serves as chairman of the Airport Minority Advisory Council.

The Chairman now recognizes Mr. Swift for his opening statement.

STATEMENT OF WILLIAM H. SWIFT, CHAIRMAN, AIRPORT MINORITY ADVISORY COUNCIL

Mr. SWIFT. Mr. Chairman, Ranking Member Thompson, and Members of the House Homeland Security Subcommittee on Transportation Security, I am a principal at Business Traveler Services, Inc. BTS is a privately-held concessionaire based out of Atlanta, Georgia.

I thank you for the opportunity to participate in today's hearing, and would like to discuss some of the issues that concessionaires like myself face on a regular basis in the airport security arena.

As a concessionaire, I am concerned about airport security, as are all those who travel daily through nearly 400 U.S. commercial airports. A breach of security that leads to a major incident significantly impacts the traffic and business for all airports, and for all of us who have businesses at these airports.

As part of my testimony, I would like to make three suggestions for the committee and Transportation Security Administration to consider: One, raising the SIDA Badge allocation limit.

I ask the subcommittee to consider raising the 25 percent allocation limitation, or implementing a reasonable minimum allocation that would allow small businesses to successfully operate in the airport arena.

Two, in showing a consistent delivery process—I recommend that the subcommittee look at ways to ensure the delivery process is subject to consistent security standards for all airports that do not unduly inhibit the ability of small concessionaires to compete and do business.

Three, in showing consistency in the processing time line for new hires—we must be able to depend on a consistently timely response from TSA and the airport, and ask the subcommittee to examine methods to ensure consistency in this process.

My comments today are focused on the impact of allocation of identification badges with SIDA badge privileges for concessionaires. It is particularly difficult for those of us who are small operators in airports having as few as one to three locations, and as a result as few as 6 to 12 employees.

In posting a 25 percent limitation on those total number of employees permitted to be issued a SIDA badge suggests that only one and a half to three employees may have a SIDA badge. This limitation is arbitrary at best, and not based on facts relative to the procedures and practices by which we are required to operate in the airport environment.

Now as we operate more often imposed by the airport, 12 to 17 hours per day, require at least two complete employee teams per day, 7 days per week on-site. A company needs opening and closing personnel, as well as floaters to address a variety of circumstances, i.e., repairs requiring an escort, product deliveries, replacing employees who call in sick or are late. The mathematical equation applied here does not work.

Under one contract I have in Atlanta Airport, we provide a number of products and services via vending and/or mechanized units. Our employee operates this array of machines through three partners: A full-time maintenance man and a clerical assistant. We all have to pitch in to keep our company a step ahead of customer service demands.

Amongst ourselves, we have asked rhetorically why does TSA view our business group as a higher risk to security of the airport.

I recommend the subcommittee consider raising the 25 percent allocation limitation, or implementing a reasonable minimum allocation that would allow small businesses to successfully operate in the airport arena.

Inconsistent handling of deliveries—another area of concern is the inconsistent handling of U.S. Postal, UPS, or FedEx packages.

Small operators frequently do not maintain an off-airport warehouse for one to two stores operating, and therefore must rely on UPS or FedEx deliveries. Some airports permit deliveries by these companies' post-security stores, while others do not permit these deliveries.

I recommend that that subcommittee look at ways to ensure the delivery process is subject to consistent security standards that do not unduly inhibit the ability of small concessionaires to compete and do business.

Inconsistent processing time frames for new hires—additional impact on the small operators, the inconsistent time frame to get hires through the TSA airport badging process, typically, this is 10 to 14 days processing, but as has been as long as 30 days. Consider that many of our new hires can ill afford to wait several weeks to get an approval, resulting in the loss of potential employees, as well as the $110 fee we are charged for each employee.

In conclusion, I thank you for allowing me to share my experiences as an airport concessionaire with the subcommittee. I understand the careful balance between maximizing security while also ensuring businesses can still operate successfully and efficiently.

I appreciate the work both the subcommittee and full committee have done in this area. Should any Members of the subcommittee have any questions for me today, I would be happy to address them.

Thank you.

[The statement of Mr. Swift follows:]

Prepared Statement of William H. Swift

May 16, 2012

Mr. Chairman, Ranking Member, and Members of the House Homeland Security Subcommittee on Transportation Security, my name is William Swift, a principal at Business Traveler Services, Inc. (BTS). BTS is a privately-held concessionaire based out of Atlanta, Georgia. I thank you for the opportunity to participate in today's hearing and would like to discuss some of the issues that concessionaires like myself face on a regular basis in the airport security arena.

As a concessionaire, I am as concerned about airport security—as are all those who travel daily through nearly 400 U.S. commercial airports. A breach of security that leads to a major incident significantly impacts the traffic and business for all airports and for all of us who have businesses at these airports. As part of my testimony, I would like to make three suggestions for the Committee and Transportation Security Administration (TSA) to consider:

1. *Raising the SIDA Badge Allocation Limit.*—I ask the subcommittee consider raising the 25% allocation limitation or implementing a reasonable "minimum" allocation that would allow small businesses to successfully operate in the airport arena.
2. *Ensuring a Consistent Delivery Process.*—I recommend that the subcommittee look at ways to ensure the delivery process is subject to consistent security standards that do not unduly inhibit the ability of small concessionaire to compete and do business.
3. *Ensuring Consistency in the Processing Timeline for New Hires.*—We must be able to depend on a consistently timely response from the TSA/airport, and I ask the subcommittee to examine methods to ensure consistency in this process.

SIDA BADGE PRIVILEGES

My comments today are focused on the impact of the allocation of identification badges with SIDA badge privileges for concessionaires. It is particularly difficult for those of us who are small operators on airports, having as few as 1–3 locations, and as a result as few as 6–12 employees. Imposing a 25% limitation on the total number of employees permitted to be issued a SIDA badge suggests that only 1.5–3 employees may have a SIDA badge. This limitation is arbitrary at best—and not based on facts relative to the procedures and practices by which we are required to operate in an airport environment. The hours we operate, more often imposed by the airport, 12–17 hours per day, require that at least two complete employee teams per day 7 days per week be on-site. A company needs opening and closing personnel, as well as floaters to address a variety of circumstances, i.e. repairs requiring an escort, product deliveries, replacing employees who call in sick or late. The mathematical equation applied here does not work.

Under one contract I have in the Atlanta airport, we provide a number of products and services via vending and/or mechanized units. Our company operates this array of machines through three partners/principals, a full-time maintenance man and a clerical assistant. We all have to pitch in to keep our company in-step or ahead of the customer service demands. The arbitrary number of SIDA badges permitted is stifling to the small operator who, through necessity of the Homeland Security proportioned allocations, is being forced into a "one-size-fits-all standard" that cannot work when it comes to the small operator. Amongst ourselves, we have asked rhetorically, why does TSA view our business group as a higher risk to the security of the airport?

I recommend the subcommittee consider raising the 25% allocation limitation or implementing a reasonable "minimum" allocation that would allow small businesses to successfully operate in the airport arena.

INCONSISTENT HANDLING OF DELIVERIES

Another area of concern is the inconsistent handling of U.S. postal, UPS, or FedEx packages. Small operators frequently do not maintain an off-airport warehouse for a 1–2 store operation and, therefore, must rely on UPS or FedEx deliveries. Some airports permit deliveries by these companies to post security stores, while others do not permit these deliveries. The impact is significant and costly for a small operator, possibly requiring that they must hire additional personnel and vehicles to be available on standby for these deliveries that can only be made and transported across the tarmac. Small operators cannot financially absorb the additional costs and remain profitable.

I recommend that the subcommittee look at ways to ensure the delivery process is subject to consistent security standards that do not unduly inhibit the ability of small concessionaire to compete and do business.

INCONSISTENT PROCESSING TIME FRAME FOR NEW HIRES

Additional impact on the small operator is the inconsistent time frame to get new hires through the TSA/airport badging process. Typically there is a 10–14 day processing, but it has been as long as 30 days. Considering that many of our new hires can ill-afford to wait several weeks to get an approval, resulting in the loss of potential employees and the fees we were charged by the airport for processing them. We must be able to depend on a consistently timely response from the TSA/airport, and I ask the subcommittee to examine methods to ensure consistency in this process.

CONCLUSION

I thank you for allowing me to share my experiences as an airport concessionaire with the subcommittee. I understand the careful balance between maximizing security while also ensuring business can still operate successfully and efficiently, and I appreciate the work both the subcommittee and full committee have done in this area. Should any Members of the subcommittee have any questions for me today, I am happy to provide my insight and will answer your questions to the best of my ability.

Mr. ROGERS. Thank you, Mr. Swift.

I recognize myself for opening questions.

Mr. Crosby, what are airports doing proactively to incorporate biometrics into their access control systems?

Mr. CROSBY. Thank you, Mr. Chairman.

It is an exciting thing that we are doing. We have voluntarily formed a consortium with airports and vendors to develop a concept of operations for biometrically-based access control systems.

Rather than being mandated by the TSA, TSA supports the fact that we are trying to do it voluntarily. Like any piece of technology, access control systems need to be replaced over time.

An example I will give you is our airport in Portland. We are about to replace our 20-year system. Right now we are heavily engaged with the free information that we are getting from airport officials at other airports who have already implemented biometrics, and those from the vendor community to get the latest technology at our airports.

Mr. ROGERS. What suggestions do you have for how both airport operators and TSA can reduce the number of security breaches that occur?

You have heard the testimony earlier today. But I would love to hear your thoughts.

Mr. CROSBY. I have.

I think that first of all TSA has made a lot of progress when it comes to breaches, in spite of maybe some of the reporting discussion that happened today. I can say, because I have been in this position since 9/11, when we all remember the times when airport concourses were dumps and many of us maybe missed flights, caused delays, hundreds of thousands dollars' worth of delay to people.

Those don't happen near as much anymore. That is because the TSA is doing a better job of communicating with their own staff and with airport law enforcement officials.

So I have seen improvement there. We have used technology to help us out.

An example of that is using closed circuit television to better identify where the anomaly happened.

The biggest area for traditional breaches at checkpoints is in the hand-off of an uncleared bag or an uncleared person between TSA officials. They are able to rectify that much more clearly and quickly now with the use of CCTV and better communication procedures.

Mr. ROGERS. Do you feel that access controls have a uniform level of security from airport to airport?

Mr. CROSBY. No, sir.

As you know, the saying in our industry is if you have seen one airport, you have seen one airport. We all have the same parts, but we are all laid out differently.

I think like any system, the best systems in the airport access control systems in the country are at airports that have proactive programs like Captain Cassidy referred to.

We have lots of programs where we rely on all badge holders to report information to us so that we can respond to it and act and deal with security instances. We award badge holders, crewmembers, concessionaires for their reporting of things.

I think those best practices that TSA has compiled, that we at airports talk about, we need to continue to spread around.

Mr. ROGERS. Thank you.

I have got to step away for a few minutes. Mr. Cravaack is going to take the chair.

I do want to let the Members know though, that later today I will be sending a letter to Administrator Pistole demanding that 100 percent of all breaches by any definition be reported up to PARIS, which is the Performance and Results Information System, the database by which they come up with processes to resolve these problems.

I will also demand that the administrator take immediate action to remedy the database deficiencies that were outlined in the testimony and the questioning by Mr. Thompson and me.

Those are inexcusable and should be remedied immediately. I am going to follow the gentleman from California's advice and recommend that if the administrator does not have the capacity to do that he needs to contract somebody that does.

With that, Mr. Cravaack, you take the chair.

Oh, and Mr. Thompson is recognized right now for any questions he may have.

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

Mr. Swift, in your testimony you suggested that TSA raise the minimum allocation of SIDA badges to vendors above the present 25 percent to allow businesses to successfully operate.

Can you explain to the committee why you raised that as a concern?

Mr. SWIFT. Primarily because if we have a small sales staff or operating staff of 10 to 12 people, 25 percent is only two or three people. When we run such a long day and 7 days a week, we have several shifts.

If we lose one person, and it takes 2.5 to 3 weeks to replace that person through the approval process, we are short. Now we are trying to figure out or jerry-rig the process in order to stay in business.

That is not acceptable to us.

Mr. THOMPSON. So in other words, the 25 percent for a small business provides what is, by that small business, an undue burden through no fault of their own from a security standpoint.

Mr. Crosby, have you looked at that?

Mr. CROSBY. Yes, sir, Ranking Member Thompson. I am glad this issue came up because I am happy to report some good news.

Over the last 2 years as chair of AAAE's security committee, and in conjunction with Airport Councils International and the TSA, we have formed a task force that has been looking at all the new security regulations that have been written since 9/11, and then modifying them to fit today's world.

One of those areas that is currently out for public review is this 25 percent rule that Mr. Swift may not be aware of. Our committee, that includes airport operators, has worked with TSA to come up with a modification to that rule that allows for relief of the 25 percent rule as long as the operator can prove a business need to have a higher percentage.

So that rule is currently under review and should be implemented in the next couple months.

Mr. THOMPSON. I guess my point is, so it is no longer 25 percent, but what is it?

Mr. CROSBY. It is whatever the vendor, concessionaire, can prove to the Federal security director is needed. Mr. Swift, as he said, we have the same case at our airport with a great concession program.

We have vendors with four operators and some with 400. It depends on where your storage area is and what times of operations you have. If you can prove that all four of those four need it, then the FSD has the authority to approve that now to 100 percent.

Mr. THOMPSON. To give you all four.

Mr. CROSBY. Yes, sir.

Mr. THOMPSON. Would that alleviate the problem we are talking about here, Mr. Swift?

Mr. SWIFT. Absolutely, but it is a matter of timing.

Mr. THOMPSON. Yes.

Mr. SWIFT. We are talking about another 6 months. We are still—it costs us money every day that we don't have the flexibility to do it right.

Mr. THOMPSON. Captain Cassidy, you suggested in your testimony that airports designate an existing employee as a security training manager.

How does that differ from your understanding of the present way things are done?

Mr. CASSIDY. Well, the way things work right now, you know, airlines have a corporate security department. They also have security personnel that are affiliated typically with the labor groups, to use an example, labor groups representing mechanics, pilots, flight attendants, dispatchers, et cetera. The bigger groups typically have a security person affiliated with them as well.

When you go to the airport, the security responsibilities alternate between being in a non-sterile area where you have security more oriented with the law enforcement folks, and then when you get to the airplane, it kind of moves over towards the airlines. So the training responsibility also moves depending on, you know, where you are in your phase of operations.

But I think the important thing is that however you get there, there has to be a team that is composed that takes into account the unique security aspects of operating an airport, operating concessions, flying the airplanes, servicing the airplanes. They need to kind of work towards coordinated——

Mr. THOMPSON. So——

Mr. CASSIDY [continuing]. On the training.

Mr. THOMPSON. So do you—is that presently your comment that that is kind of uncoordinated? Or——

Mr. CASSIDY. That is exactly right. What we have been striving for, and in fact we were involved in a working group that made a number of recommendations in the 1990s.

What we are looking for is development of a team concept so we have all the stakeholders involved with one common goal, and there is enhanced communications, you know, amongst all the stakeholders.

I think that we have a very good example of that with our safety programs, where we do have commercial air safety teams, where we have stakeholders from the manufacturers, from the labor groups, from the operators. I think that there is a tremendous power, tremendous synergy when we get them all coordinated and working in a focused manner.

Mr. THOMPSON. Thank you.

I yield back, Mr. Chairman.

Mr. WALBERG [presiding]. Thank you.

I recognize myself for 5 minutes of questioning.

Mr. Crosby, let me ask you: How frequently does your airport revoke credentials because a worker poses a threat or violates a security policy?

Mr. CROSBY. Fortunately, security violations aren't overly common. But we have a prescribed matrix of penalties for security violations.

As far as how often a security badge is revoked for a violation, it is not very often, sir. At our airport, we are the 30th largest airport in the country, I would say a couple a year.

More often, there are suspensions and retraining that happens for minor violations. But major violations we do suspend on occasion.

Mr. WALBERG. Can you discuss for us the different camera systems that the Portland International Airport has installed? Who controls the different cameras on sites, for instance?

Mr. CROSBY. Yes, sir.

The core closed circuit television system around the airport that we have enhanced over the last couple of years is the Port Authority's. But we recognize that we are in a partnership with others. We have given access to many of those cameras around the screening areas to TSA so they can better manage the customer service side of things with the line management and put their resources there.

We also work closely with Customs and Border Protection in our Federal inspection station, where they have access to those cameras. So it is a collaborative process. It really has enhanced our ability to respond and find out really what has happened when something is reported.

Mr. WALBERG. Thanks.

If one of your employees witnesses a breach of security, how can the employee report that to TSA? What is the process?

Mr. CROSBY. Well actually, our process is report it to the airport dispatch, the airport 9–1–1. That is what we train all of our badge holders on. If you see something, to use the DHS phrase, "see something, say something."

But that has been a core value at most airports for many years before that catch-phrase came out.

Every airport badge holder is required to report a security violation if they see it. We don't want them to put themselves in danger. So they call—everyone knows at our airport to call extension 4000 to get the immediate response from our law enforcement.

Mr. WALBERG. Thank you.

Captain Cassidy, thanks for being here.

Based on your experience, how do you think access control and perimeter security can be improved?

Mr. CASSIDY. Well, I think——

Mr. WALBERG. Give us your list.

Mr. CASSIDY. It is pretty big.

I think that the high level, you know, looking at it from the 33,000-foot level, we need a standard consistent approach to perimeter security. That clearly does not exist today.

In my verbal remarks, I touched a little bit on the SIDA, the identification display area. I think one of the big issues that we have is the fact that there is really a bipartite rule with respect to passenger operations and cargo operations.

Passengers have one standard, whereas there are cargo facilities, and we have no idea what kind of screening, what kind of access, what kind of perimeter security is being applied in those cargo facilities, which then enter our airspace.

That would be at the very top of my list. It is clearly in line with our desire to have one level of safety and one level of security.

I applaud Congressman Cravaack for, you know, putting the Safe Skies bill forward which tries to achieve one level of safety with regard to fatigue issues and crew duty limits. I think we should apply the same to security.

Even within the various airports, each airport has its own individual airport security program. Depending on the needs of that particular airport, the access issues change a little bit, so even the way that they get access through some of the control points, through the gates to the airplanes, differs from airport to airport.

Mr. WALBERG. Okay.

So those are the top two that you would say would go a long way.

Mr. CASSIDY. I would say one consistent approach to screening and access right across the board regardless if it is cargo or passenger would be at the very top of the list.

Mr. WALBERG. What process is in place for you to report as a pilot—report suspicious activity?

Mr. CASSIDY. Any number of ways.

First of all, typically most crewmembers have—and I don't have my crew badge with me—but typically there is a list of quick-call numbers that you have on your crew badge which takes you right to your security folks, as well as airport security.

I think that we have enough awareness, especially post-9/11, that anybody who approaches a uniformed crewmember at a dispatch desk, at a gate, will know immediately to be able to relay the information to airport security.

Mr. WALBERG. Have you ever reported?

Mr. CASSIDY. Yes.

Mr. WALBERG. What was the outcome?

Mr. CASSIDY. I have reported on any number of occasions. A very simple—and it is not particularly sexy—but, you know, I will be walking through the terminal waiting for a flight and I will notice a bag sitting in the corridor unescorted, unaccompanied.

I can't tell you how many times I have just made a simple report like that. Grabbed the CSA, who has made an announcement over the P.A. system—CSA, customer service agent, pardon me—who has made an announcement over the passenger system. If they are not able to have somebody claim the bag, then they notify airport security.

That happens thousands of times a day in all of our airports right now.

Mr. WALBERG. Okay.

Thank you. My time has expired.

I recognize the Ranking Member for her question.

Ms. JACKSON LEE. Chairman, thank you very much.

Let me thank the witnesses for their testimony that I reviewed. I was delayed at another meeting.

I want to follow the line of reasoning that I followed earlier, and I think it is imperative that we provide a safe perimeter, and also a safe opportunity for departing passengers to board. Finally for that plane to become airborne, if you will, and land at its destination.

I think that is our ultimate responsibility. You have heard in our earlier testimony and questioning how crucial that is.

Each of us has, I would say, a very large part sometimes that poses inconvenience. But I think in the midst of inconvenience, we should also be rational as well.

So I am interested in us being rational, and that my line of questioning will pose along the lines of how important it is that we all team up on this concept called securing the airport.

It is enormously difficult to hear at one of our great airports, Atlanta-Hartsfield, that people are entering it as if they are entering a carnival or they are getting away with not paying tickets for a baseball game, and two and three and four people are passing through the turnstile.

As I said, we have been discussing this perimeter and badging issue for a very long time, and we continue to have these incidents.

So let me go to you, Mr. Swift.

You are committed to making sure that your employees are credentialed. Is that not correct?

Mr. SWIFT. Absolutely.

Ms. JACKSON LEE. First of all, let me say that I am glad that we see our airports as opportunities for minority and small and women-owned businesses. I want to make sure that you know that I am completely supportive of those opportunities, and frankly believe there should be more.

So you are committed to the credentialing.

What would be—first, what is the cost that you have to pay for credentialing? What would you want to see to expedite the process?

Mr. SWIFT. Firstly, the cost is $50 for the fingerprinting and $60 for the badge. If you have been fingerprinted in the last 10 years, you don't have to get it done again.

However with the rate of turnover that takes place in any retail or food-and-beverage operation, this is a significant cost, especially when you are talking about 200 percent turnover on an annual basis.

The second part of your question, ma'am? Sorry.

Ms. JACKSON LEE. What would you like to see happening now to, one, do our chief mission, which is to secure that airport and those passengers and all others that work there, and that comports with a responsible way of dealing with your businesses, plural, meaning the concessions that are in airports?

Mr. SWIFT. Clearly, the first responsibility as a concessionaire, when I send an employee for approval for their application, I make sure the application is completely filled out. If I do my job on that end, I don't understand why it takes anywhere from 10 days to 30 days to process the employee.

The problem we have with that is on the street, if I send someone to get a job, within 2 or 3 days, they can be processed and hired.

We recognize the security issue as it relates to the airport, but it doesn't work well with us who are operating in the airport to not know exactly how long it should take us.

A day or two slip is acceptable, but when it gets in the 30-day range, it is unacceptable.

Ms. JACKSON LEE. Where do you place that burden of the time frame?

Mr. SWIFT. Well, we are not on the other side of once that application is submitted, so we don't know whether or not that time frame takes place at the airport, in terms of the fingerprint process, TSA. We just know that it takes too long.

Ms. JACKSON LEE. But the airport is where you submit the data to. Is that correct?

Mr. SWIFT. That is correct.

Ms. JACKSON LEE. Okay.

Let me—as I pursue my questions, I want to acknowledge Ed Finnegan, who has been such a great leader on a number of issues—thank him for his presence.

Captain Cassidy, let me pursue.

You would agree that flight attendants should be included in this process that is utilized by the pilots?

Mr. CASSIDY. Yes, ma'am, absolutely.

We have come out very clearly in favor of having flight attendants included in the Known Crewmember program.

Ms. JACKSON LEE. Where do you think the burden of the delay in badges may fall?

Mr. CASSIDY. Well—is this related to Known Crewmember or employee badges?

Ms. JACKSON LEE. Employee badges—if you would just give a general sense of it.

Mr. CASSIDY. You know, that is a little bit out of my area of expertise. But I know that there is a pretty significant screening process that I had to go through to get the access badges, the SIDA badges, for access at the airport that I am domiciled at.

When we turn those in, we would have to go through a whole security class, training video, and I think a 2- or 3-hour class to regain that before it even began the processing phase.

So as Mr. Swift said, that is on the other side of the fence. So I don't really have enough feeling for what happens once——

Ms. JACKSON LEE. Well, why don't you talk about the experience with the pilots?

Mr. CASSIDY. Pardon me?

Ms. JACKSON LEE. Why don't you talk about the experience with the pilots for securing that document?

Mr. CASSIDY. For securing the Known Crewmember?

Ms. JACKSON LEE. Yes. Yes.

Mr. CASSIDY. Well, it is actually a very, very effective program because what it does, it relies on existing employee databases.

All pilots and flight attendants go through a very rigorous screening and background check process. Each airline maintains employee databases.

So, every time you transit one of the Known Crewmember portals that our 20 pilot groups do, you have an instant query that is done to the pilot's active employment status with the airline. That query is continuously happening. So that combined with the other form of ID makes for a very, very seamless transit.

The best thing about it, I don't think we have really emphasized it, is that by having this alternate screening method, what it does is it allows the known travelers, the known crewmembers who are very, very well-known and background-checked to get through.

It allows TSA and all the other law enforcement agencies to focus their resources on the people they don't know about. I think that is a hugely important aspect of these advanced screening programs.

Ms. JACKSON LEE. So, you are comfortable and believe that it is a working system?

Mr. CASSIDY. Yes, ma'am.

I was at the very first airport on the very first day it stood up. From that day until right now it has worked flawlessly.

Ms. JACKSON LEE. So it should be a tool that we should look to expand.

Mr. CASSIDY. One of many tools in a multilayered security environment, absolutely.

Ms. JACKSON LEE. Let me just pose this question to Mr. Crosby coming out of Portland International Airport.

You are well aware that data for badging comes to the airport and they have a responsibility. So I would make the point that I, having lived with a lot of airports since—in my early days of being elected to the Houston City Council, I know there is a lot of work that is being done there.

But I do believe that the airports have a heightened responsibility to have a process to heighten their review so that TSA can intervene at an appropriate time and get this done.

What is your assessment of that?

Mr. CROSBY. My assessment of that, ma'am, is that airports have a lot of hardworking people that process tens of thousands of applications every day with a lot of what is on-going changing requirements that TSA has given us. We do a really good job at that the vast majority of the time.

With any document collection processor, there is always going to be an opportunity to review and check and cross-check for errors. The good news is that bad people haven't gotten through the system.

But clerical errors, a lot—there are things that we can do that are highlighted by the IG report and some airports have voluntarily done to have better cross-checks in place to make sure that the information that we are getting from the applicant is given to the Federal Government is complete.

Ms. JACKSON LEE. Mr. Chairman, if you would just yield to me a moment more, I just want to pursue this.

Do you think it is reasonable to have employees use one badge identification and allow several individuals to enter a secured area?

Mr. CROSBY. I am not sure I understand the question.

Ms. JACKSON LEE. Do you believe that it is appropriate for an employee of a concession, of the airport, under the airport's jurisdiction, because you have locked in areas where you have to badge. To have an employee that has a badge allow three and four and five employees to follow in behind them without using their badge or maybe they don't have a badge.

Mr. CROSBY. I understand.

Ms. JACKSON LEE. What are airports doing about that?

Mr. CROSBY. Yes, ma'am.

Well, first of all we are—in our training we highlight what the rules allow and don't allow. The rules do not allow for multiple badged people to enter through a gateway without swiping their badge. If you have a badge——

Ms. JACKSON LEE. But multiple people, they enter on one badge. I left my badge at home, et cetera.

Mr. CROSBY. Correct, ma'am. They have to swipe it if they have the badge——

Ms. JACKSON LEE. What is your oversight?

I mean I am disappointed—you happen to be from an airport, so don't think I am calling out Portland, but what is the oversight for that not happening?

Mr. CROSBY. The oversight is—because there are escorting provisions in the rules. You have to allow for some flexibility when you have visiting guests.

I mean, Mr. Swift knows, Captain Cassidy knows that sometimes you have to escort officials on business into the secured areas. So there has to be provisions for escorting un-badged, un-badged people.

The way the system works without having bad things happen is that you have to hold people accountable. That is what we do at our airport.

We have cameras at key access points. Whenever we determine there has been a piggybacking violation, as this is called, we put a penalty on that person for doing it.

Ms. JACKSON LEE. Do you report it to TSA?

Mr. CROSBY. Absolutely. All of our security violations that are reported to us, we give TSA full access to.

Ms. JACKSON LEE. All right.

I yield back, Mr. Chairman.

Thank you.

Mr. CRAVAACK [presiding]. The gentlelady yields back.

I will yield myself 5 minutes.

Thank you very much for being here today, what I consider extremely important, obviously from previous testimony regarding the security of our airlines.

I would also like to recognize Ed Finnegan again, from the 8th District of Minnesota. Thank you for taking even more time away from your family and being here today.

So thank you very much.

Captain Cassidy, with all the experience and hours that you have in flying in many different airports throughout the country, if not around the world, you mentioned in your testimony examples of al-Qaeda basically probing our security measures in trying to gain access to the shadow of the aircraft.

What procedures do you think, as a first-line observer, that need to be implemented in ensuring that the shadow of the aircraft remains secure?

Mr. CASSIDY. Well, I think that you know a robust criminal history and background check, including fingerprinting is an absolute requirement to make sure that we have as much data available for potential threats to the aircraft.

The other thing I think that we have to recognize is that we are never going to live in a world where we are 100 percent risk-free with regard to security issues. It is just that world does not exist.

So what we have to do is apply multiple layers of security. That comes with prescreening methods, working with our agencies, using intelligence-based methods just as they did when they were able to intercept a potential terrorist who was basically going to have a little bit of a clone of the underwear bomber.

Fortunately, they were able to identify the threat and thwart it offshore before it even got to the airplane shadow. I think that probably one of the biggest ways that we can help to mitigate that security threat is to recognize the fact that we have a tremendously talented pool of folks that are in our airports right now. They are the operators, they are the pilots, they are the flight attendants.

If you operate an airplane day-in, day-out, if you staff an airplane day-in, day-out, even though you can't quite identify something that is a little bit different, you know that something is different.

By having a coordinated approach, by having stakeholder teams that work together, identify security breaches, do a data-driven analysis of what caused those breaches, hopefully we can take a more kind of data-driven approach to enhancing our security environment; rather than just taking an ad hoc one that looks at the last time that the caterer inadvertently got in the airplane. Try to figure out what went wrong after it happened.

What we need to do is develop a system that looks at precursors to security breaches and try to identify those things before they get to the airplane shadow.

I think that as we have with safety systems—we have something called the Safety Management System which aggregates all these different safety events, safety data, and looks at precursors. We look at one kind of coordinated way of enhancing safety.

We haven't quite got there yet with security, but I think that is probably where we need to go next is to take an enlightened view towards security, and look at security management systems which incorporate all those different layers of safety.

Of course, the very last layer of safety, and I applaud you for your support of that, is the Federal Flight Deck Officer program. When all else fails, it is really extremely reassuring to know that there is a pilot in the front who is prepared to defend that airplane and keep it from being used for very, very evil intentions.

So all those things work in tandem, not any one solution is the answer. But a coordinated kind of more kind of data-driven approach is clearly the way to approach that.

Mr. CRAVAACK. I would tend to agree. The information that I am receiving as well, having layered approaches of security is obviously the way to go.

At the same time making sure that we use a risk-based analysis and identifying those that are safe risks, those that are either unknown or potential risks. I would strongly agree with that.

One point you made, and I wanted to make sure that this does not go unnoticed, what would you consider the last line of defense of any passenger aircraft or cargo aircraft for that matter?

Mr. CASSIDY. That would be the Federal Flight Deck Officer program. We are very pleased to be involved in the incipient—the development of the program. We are very proud supporters of it. We continue to be enthusiastic supporters of the Federal Flight Deck Officer program.

Mr. CRAVAACK. I would tend to agree with you, Captain.

Thank you.

Also, Mr. Crosby, you did mention that when you do report to TSA—what you considered a breach of security, you report to the TSA.

Have you had satisfactory response from the TSA?

Mr. CROSBY. Yes, we have, Congressman.

TSA has an open book to look at all security violations that we investigate. Every time we have a reported violation, our Department investigates it and makes a determination of whether there has been a violation and issues the proper penalty, a due process for all things. We allow TSA to see that whole process.

Mr. CRAVAACK. Excellent.

Thank you very much, sir.

My time has expired.

I will recognize Mr. Davis from Illinois.

Mr. DAVIS. Thank you very much, Mr. Chairman, and I thank our witnesses for being here.

Mr. Crosby, in your testimony you made several references to the importance of the airport's need to leverage local experience, expertise, and knowledge.

How do you envision that being phased into a Federal system cooperatively for use that may be applied in many different or in several different locations?

Mr. CROSBY. Well, Congressman, I think it is—the system that we have had in place at airports has evolved over time, and before Federal credentialing was necessary in other transportation venues, and it has worked well.

I will give you two examples.

One, we get the criminal history record information back from the Federal Government that may not be fully complete and we locally adjudicate it.

Meaning if there is a person who has been arrested for a crime, but the information we get from the Federal Government doesn't show a conviction, we are able to meet with the applicant, verify the information, help them get the court documentation they may need, and really verify whether this person is a threat and whether they meet the threshold for getting a badge.

Second, I think that the local application is that all access control systems—while our badge colors may look the same—the captain and I have, we work at the same airport, most airports tailor access to what that person needs to do their job. That is what is critically important.

With the advancement in access control systems, an airport may have 100, 1,000 different doors in and around the airport, but you only get access to the ones that Alaska Airlines needs not the ones that Delta. That makes for people having less of an opportunity to do bad things if we control their access to do their job.

Mr. DAVIS. Captain Cassidy, and Mr. Swift, both, how do you view your interactions with Federal or local authorities in a cooperative way, that would meet both the needs that represent say, the needs of pilots in a sense, and the needs of vendors in a sense?

How does that work to become more effective as well as more facilitative of your needs?

Mr. CASSIDY. Do you want to go first?

Mr. SWIFT. Well, one side of that, of course, from a concessionaire's perspective is try to help. How can we do this better, faster, easier, and make sure it is accurate?

One thing that we are entertaining is the possibility of all our employees fill out an application on-line. That will help to guarantee that there is no difference in what is stated on the application and what the applicant wrote.

Unfortunately, many of the applications are done by hand. We can understand why there are problems with understanding certain numbers and letters—don't look the same to everyone.

So we think that that is something we would suggest is a simple software package that allows an employee to step up to a computer, fill out the application, and now we can be sure that everyone is looking at the same document.

We think that, in itself, would help as part of the process. We think there is a cooperative effort on everyone's part to do it.

It is just that it is a massive process where you are processing over half a million applications a year. It is significant.

Mr. CASSIDY. I picked up on one word in particular, and that was collaborative. I think that that is the really key ingredient to a successful relationship is working collaboratively together with the various law enforcement agencies, both at the Federal level and also the local level.

We have a good relationship, especially with the program managers for the Federal Flight Deck Officer, with TSA officials tasked with various aspects of security. The local relationships are really where the rubber hits the road, and that really varies from airport to airport.

We have dedicated committee volunteers. We have over 400 volunteers working in our safety and security structure, many of them have previous law enforcement backgrounds. So they have much more of a conduit to kind-of relating to the local enforcement officers.

The challenge is really the sharing of intelligence, the sharing of data. That is where I would like to see some improvements where we have a better sharing of information which indicates what the security threats are. We are going to continue to work in that effort.

Mr. DAVIS. Thank you, gentlemen, very much. I appreciate your being here.

I yield back, Mr. Chairman.

Mr. CRAVAACK. The gentleman yields back.

The witnesses—thank you very much. We have a second round of questions if you would be so inclined.

I would like to recognize the Ranking Member.

Ms. JACKSON LEE. Mr. Chairman, thank you very much and to the witnesses.

Let me pose again, to Captain Cassidy, how important the airline crew, captain, flight attendants are to be trained to report breaches or to—and I think there is a balance.

You are there to serve. We realize that.

You are there to promote the brand of the airline. We appreciate that.

But how important are the eyes and ears of those who are familiar with airports?

Mr. CASSIDY. Well, I think it is incredibly important. I think, you know, looking at first, the pilots and the flight attendants, the airplane crew—you notice that I talk about us as one cohesive crew, not the pilots separated by the flight attendants because, really, especially when the planes pushes back from the gate, they are really the eyes and ears of the activity in the cabin.

Their ability to communicate irregular situations to us, to indicate potential security threats, allows us to take appropriate action, lock down the flight deck, and decide whether or not we have to take the next step and consider diverting the airplane to a location to get on the ground as expeditiously as possible to try to ameliorate some of the threat, try to reduce the threat and avoid taking it further down the road.

Now, expanding that tight circle of trust that exists between the pilots and the flight attendants, we also have mechanics, service employees that service the airplanes, that man the gates.

In fact when you are on the ground, your ground security coordinator is typically the lead customer service agent for the airline before the cabin door shuts and you push back.

So it is incredibly important that we figure a way to work as efficiently and as collaboratively as possible.

Before I came over here, I pulled up some statistics and I think the Bureau of Transportation statistics said that there was about 480,000 airline employees employed in the United States in 2010.

When you look at the component that you have very well-known, very well-trained employees that form a significant majority of that, you have a massive talent pool of folks that can work together and become the eyes and ears with respect to potential security threats.

Ms. JACKSON LEE. Do you feel that you have a direct or immediate access to report a breach that you have seen?

Do you know what to do? If a captain—you could be coming through and you see three people go through a door. You know, there was a badge——

Mr. CASSIDY. Right.

Ms. JACKSON LEE [continuing]. And the door is open and three people go through.

Have we made our airline crews sensitive enough—they are going about their business. They may be rushing to their flight.

Is there an easy number, an easy call to make to say this is what I saw at door number 2468?

Mr. CASSIDY. 9–1–1. You can go to any place in any airport, any concession——

Ms. JACKSON LEE. Is that a 9–1–1 to the airport or a 9–1–1 to police?

Mr. CASSIDY. Typically it goes—it depends on the airport and I think Mr. Crosby would back me up on this, but it is going to get routed fairly expeditiously.

You can also go to a concession stand and say you have an emergency. They are going to have law enforcement there quicker than you would probably realize because of the way that they are stationed around the terminals.

Ms. JACKSON LEE. So you would feel comfortable in doing that because I would imagine you would see three uniformed concession—I mean I call him by his name, but different things that are in the airport and they look legitimate.

Do you keep going or do you call 9–1–1?

I mean I think that is a very sensitive question. We need to try to understand so we can——

Mr. CASSIDY. Right.

Ms. JACKSON LEE [continuing]. Improve our circumstances.

Mr. CASSIDY. We have 53,000 members that we represent. We are the biggest pilot union in the world. I am very, very confident that the vast, vast majority of those members would feel the same way that I would, and that is where we would say something.

I can give you an example. One of the times I was flying I was walking around doing my pre-flight on the ramp, and I noticed that one of the service folks, the rampers that carry the bags and whatnot, had no identification on him, none.

So I went up to the individual and I said, "Do you have an airport ID? Do you have a SIDA badge?"

Fortunately he pulled one out of his pocket and put it around his neck and thanked me.

But had he not had that, the very first thing I would have done was gone to his supervisor and said, "We have somebody walking around in a sterile area, on the ramp, around all these airplanes and we have no idea who that person is."

I am very confident that the flight attendants that I work with and the pilots and the mechanics would do likewise.

Ms. JACKSON LEE. We need to just continue to reinforce that is what——

Mr. CASSIDY. Yes, ma'am.

Ms. JACKSON LEE [continuing]. Is what we need, to make it clear or approving that that be done.

Do you think that the airlines themselves, the corporate entities, need to recognize that value that you have in doing that and reinforce that in their employees as well, and airports?

Mr. CASSIDY. Yes, ma'am.

I can't emphasize enough how important it is for the airlines and the airports to really understand the talent and the potential that you have when you empower all those different employees to be part of the stakeholder team, be part of the team that can make a difference in the security systems at that particular airport.

I think we have already done that with safety systems, as I said before. I think it is time to look at the next frontier and apply that same kind of standard to security systems.

Ms. JACKSON LEE. Mr. Chairman, I thank you for indulging.

Let me—I just want to finish this line of reasoning.

Captain, do you also believe it is important, because I would like to work with the Chairman and I would like to work with this Chairman as well, because of his expertise, that cabin security. You know, we have gotten comfortable because—and I only use that term comfortable—but we always cite we have got the reinforced door and we have got the on-deck pilots, which I appreciate.

That—but your responsibility is make sure that plane stays up and not down, even though you may be equipped to come running out of there.

I know you would like not to run out of there. We have had a number of incidences. One in particular that deals with the pilot.

But the point is my concern is that we have comfort with, well, the brave passengers will jump up.

Do we need to look at cabin security as well as an issue?

Mr. CASSIDY. I think it is an evolving thing. We have to understand what the potential threats are.

I think that with regard to the security behind the flight deck door, we go through recurrent training annually. Airlines typically do it as an integrated crew.

We participate in security training with the flight attendants, and discuss things such as what do you do if you find an unidentified suspicious-looking device sitting in an overhead bin? What happens if you have an unruly passenger? How do you communicate it to the pilot, and everything in between?

So I think that the training is there. But am I going to tell you that it couldn't get better? Absolutely not, it can always get better. But I am very pleased to say that we work very well together.

Ms. JACKSON LEE. We would like to help you get better.

I understand that we have got a few of friends that are engaged in negotiations with their pilots, in particular United. I would like to get a briefing.

I, frankly, believe that when you have an extended negotiation that you can't resolve you really do raise a question about focused effectiveness. I think pilots, flight attendants, being right on the airplanes are so important that any delayed negotiations.

So how can we ramp that negotiation up as they proceed to try to settle this issue?

Mr. CASSIDY. Ma'am, I would be happy to give you a brief on what the status is right now of the negotiations. I think that I would be remiss if I also didn't point out that I think it is a tribute to the professionalism and the quality of the men and women that we have flying for us that despite the distractions of all these negotiations we still fly the safest skies in the world and we still have the safest air transportation in the history of the world right here, right now.

Ms. JACKSON LEE. I absolutely want to get that on the record. That is why I believe they need to ramp up their efforts and get this resolved, so that the men and women who are at this high level can not only fly airplanes, but be quick eyes to help the traveling public.

I know the Chairman has been very indulgent. Here is my last point, Mr. Chairman, as I conclude.

I also believe judgment should be key. Let us see—as you well know, you might have heard the story of a 2-year-old toddler that was on the no-fly list.

I am really going to point back at our good friends, captains, you are—he or she is the king of that flight, and rightly so. I would just ask publicly that a 2-year-old on a no-fly list, let us report it and let them fly.

Obviously, we have had a series of issues on the no-fly list, and I guess I am going to ask on the record—this will not be—I would want a response back—what is the penalty for an airline who indicates that a toddler could fly and their name is on a no-fly list?

Because everyone always says what the FAA is going to do, they cite agencies that are probably not even relevant, but that is what they know to cite. I think that gives all of us a bad name, if we have to clarify the no-fly list.

But if a toddler has got their name on the no-fly, in this incident the pilot or the airline—let us not say pilot—the airline made the toddler get off. Obviously they couldn't get off by themselves. So I am really concerned about that.

I will conclude on this note. I believe that what we have discovered in this hearing is a fracture that has to connect the Transportation Security Administration as a front line in receiving all reports on breaches, every one of them.

I appreciate, Captain, that it will be 9–1–1, but then the airport, if they have 9–1–1—and it may be an issue that is relevant for 9–1–1. But that 9–1–1 call and the response, that should go to the TSA.

Mr. Crosby, I believe I didn't get the next sentence from you as to whether or not the airport is reporting this to TSA. So let this be a statement from me as the Ranking Member on this committee.

I know that I want to work with the Chairman and Chairman Cravaack, who is here, that we have got to have a zero tolerance on missing the reporting of any breach that is occurring in the Nation's airports, to make good on our promise to secure America.

I think that should be a demand out of this particular hearing. As I asked Mr. Sammon, Assistant Secretary Sammon, to begin doing that now and communicating with airports, and if you have to go back through old dusty, rusty records that happen to be 2 months old or a year old, we have to start where you can find your records.

Those breaches need to be reported. All of our workers need to feel free to do so.

Although we don't want to compromise security, we need to work with our small businesses, and TSA needs to develop a time line that does not compromise security, but in fact responds to some of the concerns that have been expressed in this hearing.

Mr. Chairman, you have been overly indulgent. Thank you very much. I yield back to you.

Mr. CRAVAACK. I thank the gentlelady.

I thank the witnesses for their testimony today and the Members' valuable questions as well.

Members of the committee may have some additional questions for the witnesses, and we ask you to respond to these in writing.

The hearing record will be open for the next 10 days.

Without objection, so ordered.

The committee stands adjourned with your thanks.

[Whereupon, at 12:28 p.m., the subcommittee was adjourned.]

○