

SECURING OUR SKIES: OVERSIGHT OF AVIATION CREDENTIALS

HEARING BEFORE THE SUBCOMMITTEE ON TRANSPORTATION AND PUBLIC ASSETS OF THE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM HOUSE OF REPRESENTATIVES ONE HUNDRED FOURTEENTH CONGRESS SECOND SESSION

FEBRUARY 3, 2016

Serial No. 114-103

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



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

U.S. GOVERNMENT PUBLISHING OFFICE

23-402 PDF

WASHINGTON : 2017

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

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

JOHN L. MICA, Florida	ELIJAH E. CUMMINGS, Maryland, <i>Ranking</i>
MICHAEL R. TURNER, Ohio	<i>Minority Member</i>
JOHN J. DUNCAN, JR., Tennessee	CAROLYN B. MALONEY, New York
JIM JORDAN, Ohio	ELEANOR HOLMES NORTON, District of
TIM WALBERG, Michigan	Columbia
JUSTIN AMASH, Michigan	WM. LACY CLAY, Missouri
PAUL A. GOSAR, Arizona	STEPHEN F. LYNCH, Massachusetts
SCOTT DESJARLAIS, Tennessee	JIM COOPER, Tennessee
TREY GOWDY, South Carolina	GERALD E. CONNOLLY, Virginia
BLAKE FARENTHOLD, Texas	MATT CARTWRIGHT, Pennsylvania
CYNTHIA M. LUMMIS, Wyoming	TAMMY DUCKWORTH, Illinois
THOMAS MASSIE, Kentucky	ROBIN L. KELLY, Illinois
MARK MEADOWS, North Carolina	BRENDA L. LAWRENCE, Michigan
RON DESANTIS, Florida	TED LIEU, California
MICK, MULVANEY, South Carolina	BONNIE WATSON COLEMAN, New Jersey
KEN BUCK, Colorado	STACEY E. PLASKETT, Virgin Islands
MARK WALKER, North Carolina	MARK DESAULNIER, California
ROD BLUM, Massachusetts	BRENDAN F. BOYLE, Pennsylvania
JODY B. HICE, Georgia	PETER WELCH, Vermont
STEVE RUSSELL, Oklahoma	MICHELLE LUJAN GRISHAM, New Mexico
EARL L. "BUDDY" CARTER, Georgia	
GLENN GROTHMAN, Wisconsin	
WILL HURD, Texas	
GARY J. PALMER, Alabama	

JENNIFER HEMINGWAY, *Staff Director*

DAVID RAPALLO, *Minority Staff Director*

MICHAEL KIKO, *Staff Director, Subcommittee on Transportation and Public Assets*

ARI WISCH, *Counsel*

MICHAEL DING, *Counsel*

WILLIE MARX, *Clerk*

SUBCOMMITTEE ON TRANSPORTATION & PUBLIC ASSETS

JOHN L. MICA Florida, *Chairman*

MICHAEL R. TURNER, Ohio	TAMMY DUCKWORTH, Illinois, <i>Ranking</i>
JOHN J. DUNCAN, JR. Tennessee	<i>Member</i>
JUSTIN AMASH, Michigan	BONNIE WATSON COLEMAN, New Jersey
THOMAS MASSIE, Kentucky	MARK DESAULNIER, California
GLENN GROTHMAN, Wisconsin, <i>Vice Chair</i>	BRENDAN F. BOYLE, Pennsylvania

CONTENTS

Hearing held on February 3, 2016	Page 1
WITNESSES	
Mr. Darby LaJoye, Deputy Assistant Administrator, Office of Security Operations, Transportation Security Administration, U.S. Department of Homeland Security	
Oral Statement	5
Written Statement	8
Mr. John Roth, Inspector General, Office of Inspector General, U.S. Department of Homeland Security	
Oral Statement	17
Written Statement	19
Ms. Margaret Gilligan, Associate Administrator for Aviation Safety, Federal Aviation Administration, U.S. Department of Transportation	
Oral Statement	32
Written Statement	34
Ms. Kathleen M. Carroll, Vice President, Government Affairs, HID Global (On Behalf of the Security Industry Association "SIA")	
Oral Statement	38
Written Statement	40
APPENDIX	
TSA's responses to the Committee's Questions for the Record, Submitted by Chairman Mica	58
TSA Warehouse Information by Quarter FY12, Submitted by Chairman Mica	71

SECURING OUR SKIES: OVERSIGHT OF AVIATION CREDENTIALS

Wednesday, February 3, 2016

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TRANSPORTATION AND PUBLIC
ASSETS,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The subcommittee met, pursuant to call, at 1:05 p.m., in Room 2154, Rayburn House Office Building, Hon. John L. Mica [chairman of the subcommittee] presiding.

Present: Representatives Mica, Duckworth, and DeSaulnier.

Mr. MICA. I call this hearing of the Transportation and Public Assets Oversight Subcommittee to order, and I welcome everyone this morning.

Without objection, the chair is authorized to declare a recess at any time. We do expect some votes pretty quickly into the beginning of this session, so we'll try to get our opening statements made, and then we will hear from our witnesses. And the order will be after we've heard from all the witnesses to go back and have questions offered to the witnesses.

So I'll start with my opening statement. And, again, welcome, everyone.

We have an important responsibility in transportation oversight, and that's to make certain that the laws and all of the caveats that we set forth for public agencies, particularly for security and safety, are complied with by agencies. And the purpose of this hearing is 15 years after 9/11 we want to look at credentialing, we want to look at vetting of employees, and we want to look at what poses the biggest risk as far as security to our Nation's aviation system.

Unfortunately, even 15 years—2001, this is 2016—15 years later we still seek a system that has not complied with the laws that we have passed multiple times with the requests we've had, and we see failures. One of the biggest failures is the most recent report that we had. And the DHS, Department of Homeland Security inspector general found that 73 individuals with links to terrorism passed TSA's vetting process. They were not properly vetted.

These are people that work at our airports. These are people that have access to aviation equipment, to airplanes. Even TSA employees are not properly vetted.

And, unfortunately, we've also found through that report that tens of thousands of incomplete records are even lacking full names. They had 14,000 immigrants listed in the database that did

not have alien registration numbers, and 75,000 of these records lacked passport numbers. Again, this is not acceptable.

When we passed the aviation security bill, and in subsequent legislation I tried to get a—we used to have a folded piece of paper for an airline pilot license. An airline pilot has access to the controls, flying the plane. I can tell you today, after numerous enactments of laws and edicts and meetings, we still have a pilot's license. And I borrowed this one from our ranking member. She's a pilot, Ms. Duckworth.

We asked that the pilot's license have a photo of the pilot on it. The only photo on this license are the Wright brothers, Orville and Wilbur. Orville and Wilbur, I blew it up here. Okay? It's a joke.

We asked that this also has some biometric capability. Anything in your wallet has a better electronic strip and capability than this license.

Now, you say it's too difficult to do with the pilots that we have. This is a Mickey Mouse. This happens to be Minnie Mouse pass to Disney World, and I borrowed this. My wife was there the other day with her sister visiting. They take your thumb print, and they know when you enter, who enters, who leaves. This is Minnie Mouse, and this is Mickey Mouse, the FAA pilot license.

So this is what we have, people going into the airports, people who, secure areas, either working for TSA or airports, not properly vetted, a responsibility of TSA. We have pilots who are flying planes, we don't know who they are. You cannot tell.

Again, the frustration level has just peaked with me, because time and time again we've gone in, we've passed edicts, laws, for compliance.

Now, this particular Mickey Mouse, Disney World pass has a biometric for a thumb, and that we're told by FBI it possibly could be compromised. But we have nothing. I've tried to get not only a thumb, but also iris, and it took a dozen years to get a standard in place. We'll find out where they are. Because between iris and thumb, which some European nations, some of the defense agencies, some nuclear facilities, some other government facilities, both in the United States and outside, have the capability to do both, and then we're sure of who is entering and who is leaving. But I'm telling you, this is one of the most frustrating things that we've seen.

We've seen examples of employees with accomplices, for example, in New York, were able to smuggle more than 150 guns on half a dozen flights between Atlanta and New York City.

Just a few weeks ago, the FAA suspended a program allowing safety inspectors to bypass TSA checkpoints after one was caught with a firearm in a bag he was carrying.

So, again, we have examples of the Transportation inspector general opened nearly 70 pilot license fraud cases since 2011, just the last few years, including a foreign national who hacked into FAA's record system, stole the pilot's identity, and to illegally obtain a license and crashed an airplane.

We had recently one of our oversight agencies found hundreds and thousands of IDs missing, not accounted for, SIDA badges, TSA badges, airport identity badges, badges that some of the offi-

cers wear, everything you could imagine stolen or missing or unaccounted for. None of this is acceptable.

So we have other examples we can cite where it has been done, both the private sector, other government agencies, Canada to the north. And, again, I cited Disney World as a good example.

So with that, I will yield to our ranking member, Ms. Duckworth, welcome her, and give her back her FAA Mickey Mouse pilot license with Orville and Wilbur. And you are much better looking than either of those dudes.

I yield.

Ms. DUCKWORTH. Thank you, Mr. Chairman. And I'm also much more alive as well.

Mr. MICA. I visited their gravesite, and they are there, they're very much dead.

Ms. DUCKWORTH. Yes. Well, thank you so much for holding this hearing, Mr. Chairman. I am somewhat astonished that the inspector general for the Department of Transportation could not find the time to be here. But we'll deal with that at another time.

Our Nation's 440 airports are complex mazes of public and secure spaces. Chicago O'Hare, for example, which served more than 34 million passengers in 2014 alone, has 8 active runways, 189 gates, nearly 23,000 parking spaces, and approximately 167,000 square feet of concession space.

In addition to being responsible for screening all passengers who come into the airport to board a flight, the TSA must oversee the procedures that airports implement to ensure that all controlled areas, such as passenger loading areas, cargo and baggage handling areas, and perimeter areas, are accessed only by authorized personnel.

The first step in this process is identifying the individuals who should have access to secured areas and the level of access that they should be given.

Now, our Nation has different models for issuing access credentials in the various transportation modes. In the aviation realm, each airport issues its own set of access credentials. And before an airport can issue a badge allowing access to a controlled area, a person to be credentialed must be screened against terrorism databases and pass a check of lawful authority to work in the United States conducted by the TSA using data collected by each airport.

They must also complete a criminal history records check. This check is then conducted by the FBI using fingerprints and data collected by the airports, but the results are adjudicated by each individual airport to determine whether an individual has a disqualifying conviction. The Department of Homeland Security's Office of Inspector General has repeatedly found numerous flaws and lapses in the management of this complicated, multiagency process.

In 2011, the IG determined that airports issued badges to individuals despite omissions and even inaccuracies in the records used to conduct the background checks. In some cases, airports even issued badges to individuals who have not undergone security threat assessments at all.

This finding was troubling enough, yet what truly concerns me is that just last year, 4 years after that very alarming 2011 finding, the DHS inspector general found that airports continue to lack ac-

curate quality controls necessary to ensure criminal background checks are properly adjudicated.

They found systemic problems with the credentialing process also. For example, unlike tourism screenings, which are continually updated on a near real-time basis, criminal records checks are conducted only once every 2 years. Between checks, airports have to rely on the willingness of the credentialed person to self-report any disqualifying arrests or convictions. This dangerous loophole must be closed.

Officials have also uncovered airport employees illegally using stolen or fraudulent credentials. In 2007, more than 100 vendor employees at O'Hare were caught using stolen badges to access secured areas at the airport. In one instance, an uncleared individual rummaged through a box of active security badges to select one that looked most like him and matched his likeness.

Other incidents have involved cleared personnel who misused the access granted to them. Following a 2014 incident involving the smuggling of over 100 guns, some of which were loaded onto multiple flights between Atlanta and New York, TSA asked its Aviation Security Advisory Committee to recommend ways of strengthening the control of employees' access to secured airport areas. This committee made 28 recommendations in April. Fewer than half of those have been implemented.

America's airports are vital hubs that support billions of dollars in commerce and connect Americans from coast to coast. Yet, their importance also makes them high-value targets to our enemies that seek to harm Americans, weaken our economy, and instill fear throughout the populous. The front gates to our Nation's commercial aviation system must be worthy of all they defend. We must ensure that anyone passing through the gates, including airport employees, do not pose a threat to our Nation's security.

I look forward to hearing from our witnesses today on how TSA will strengthen its coordination with airport authorities across the country to implement critical security recommendations and dramatically enhance how we control access to secured areas.

Congress has an important role to play in this effort, and if additional authorities over oversight actions are needed, I would like to use this afternoon to examine those potential reforms.

Again, I thank the chairman for this very timely and important hearing, and I yield back.

Mr. MICA. Well, thank you. And the title of this, I guess, was originally "Securing Our Skies: Oversight of Aviation Credentials." I think a more fitting title, after hearing our opening statements, would be "Aviation Credentials in Chaos." That might sum it up better. I thank you for your opening statement.

And we will hold the record open, with your agreement, for 5 legislative days for members who would like to submit a written record.

Mr. MICA. And as I said, we'll probably be in and out because of the vote schedule this afternoon.

I would like to now recognize our panel of witnesses. I'm pleased to welcome Darby LaJoye, deputy assistant administrator for the Office of Security Operations at the Transportation Security Administration within DHS; the Honorable John Roth, who is the in-

spector general for the U.S. Department of Homeland Security; Margaret Gilligan, and she is the associate administrator for aviation safety at the FAA within the Department of Transportation. Welcome back.

Kathleen Carroll, who is vice president of government affairs at HID Global, speaking on behalf of the security industry.

So those are our witnesses. Some of you have been here before. I know the inspector general has.

This is an investigation in an oversight subcommittee of Congress. We do swear in all of our witnesses. If you'll stand now, please, raise your right hand.

Do you solemnly swear or affirm that the testimony you are about to give before this subcommittee of Congress is the whole truth and nothing but the truth?

And all the witnesses, the record will reflect, answered in the affirmative.

Let's go first, from TSA representative, Mr. LaJoye.

You're welcome and recognized, sir.

We do give you about 5 minutes. If you have additional information you want submitted for the record, just request and we'll put it in.

Thank you.

WITNESS STATEMENTS

STATEMENT OF DARBY LAJOYE

Mr. LAJOYE. Good afternoon, Chairman Mica, Ranking Member Duckworth, and members of the subcommittee. Thank you for the opportunity to appear before you today to discuss TSA's role in airport access control and aviation worker credentialing.

TSA ensures airport access control is executed in partnership with airports, air carriers, and other Federal agencies. Collectively, we employ a risk-based approach that includes vetting and credentialing of airport and airline employees, development and execution of security plans, TSA inspections, assessments, and testing of access control, along with random screening of aviation workers.

TSA requires airport and airline employees to successfully complete a security threat assessment prior to receiving an access credential to a secure area of an airport. The assessment includes a daily check against the Terrorist Screening Database, ensuring there are no known ties to terrorism when applicants apply for a credential and throughout the term of a worker's airport employment.

TSA also verifies all individuals have lawful presence and have not committed a disqualifying offense in the past 10 years. TSA recognizes the value of conducting frequent criminal history record checks and has established a requirement for airports or airlines to do so every 2 years for all credential holders. Later this month, we will begin to a pilot a new FBI automated capability called Rap Back, providing employers with current information on criminal activity committed by credential holders.

We recognize the value of automated access to additional intelligence-related data to inform TSA's vetting decisions. Working

closely with DHS and the interagency partners, we've recently received approval for automated access to additional data addressing a key IG recommendation. We expect to begin receiving automated access in the coming weeks.

While TSA is responsible for conducting vetting of aviation workers, airport operators are responsible for issuing and managing the credentials that allow an individual access to airports' sterile or secure areas. TSA requires airport operators to conduct recurring comprehensive audits of all airport-issued credentials and to maintain records of those audits for 1 year, subject to TSA inspection.

Individuals who are responsible for reporting lost or stolen credentials, and airport ID systems must be capable of immediately denying access to any lost or stolen credentials. If the percentage of unaccounted-for or lost credentials reaches a certain threshold, the airport must reissue all credentials in that access category.

TSA also requires airport operators to control entry to nonpublic areas of the airport and provide for detection and response to unauthorized presence in these controlled areas and to aircraft. To enforce these standards, our inspectors conduct assessments and audits and employ a progressive methodology that provides for a range of enforcement measures, from helping stakeholders with corrective actions to issuing fines.

We've made progress in addressing the insider threat at America's airports, which were highlighted by the Atlanta gun-smuggling incident in 2014. In addition to new vetting and regulatory measures, TSA and airport authority resources are deployed on a random basis to screen airport and airline workers throughout the day. In 2015, we increased the number of employee screenings from 2 million to nearly 13 million, and 90 percent of airports have reduced access points, resulting in nearly 500 fewer nationwide.

Finally, under the leadership of Administrator Neffenger, TSA has renewed its commitment to security effectiveness. In late May, after reviewing the DHS IG's covert testing results, TSA began implementing a range of measures to address the shortfalls noted. We have refocused on our primary security mission, retrained our entire workforce, improved processes and procedures, enhanced our technology, implemented new measures of effectiveness, and analyzed systemic issues. Notably, we have begun to employ a doctrinal approach to counterterrorism leading to screening improvements across the agency.

In January, we began to send all new hire officers to basic training at the TSA Academy at the Federal Law Enforcement Training Center. This will drive consistency, professionalism, dedication, and connectedness to a common agency culture. Also, thanks to the help of Congress, we halted FY '16 staff reductions, providing appropriate officers to pursue screening effectiveness.

The administrative intent is to place mission first, invest deliberately in a well-trained and disciplined workforce, and deliver mission excellence. We are confident that the agency is better positioned today to deter, detect, and disrupt threats against our aviation system, and we will continue to pursue a range of improvements to protect the traveling public.

I am proud to represent TSA's hard-working nationwide team of officers, inspectors, explosive specialists, air marshals, and a dedicated network of professional staff who support them.

I look forward to answering your questions.

[Prepared statement of Mr. LaJoye follows:]

**Statement of
Darby LaJoye
Deputy Assistant Administrator
Office of Security Operations
Transportation Security Administration
U.S. Department of Homeland Security
before the
United States House of Representatives
Committee on Oversight and Government Reform
Subcommittee on Transportation and Public Assets
February 3, 2016**

Chairman Mica, Ranking Member Duckworth, and members of the subcommittee, I am pleased to appear before you today to discuss the Transportation Security Administration's (TSA) role in airport access control and, in particular, aviation worker credentialing at our Nation's airports.

TSA's mission is to protect the Nation's transportation systems to ensure freedom of movement for people and commerce. TSA ensures that airport access control is properly executed in a joint partnership among TSA, airports, air carriers, and other Federal agency partners. To fulfill this critical mission, TSA and stakeholders employ a risk-based security approach that includes: vetting and credentialing of airport and airline employees prior to being granted unescorted access to secure and sterile areas of the airport; the development and execution of security plans as required by Federal regulations; TSA inspections, assessments, and testing of access control systems and processes at airports; and random screening of aviation workers throughout their work day. This multi-capability approach helps to ensure that

resources are applied effectively and efficiently to have the greatest impact in reducing risk associated with insider threat.

TSA takes insider threats very seriously and has made progress in addressing such vulnerabilities in America's airports, which were highlighted by the gun-smuggling incident at Hartsfield-Jackson Atlanta International Airport in December 2014. Responding to the Secretary's directives subsequent to that incident, TSA implemented a variety of measures to include: establishing a requirement for airports and airlines to conduct fingerprint-based Criminal History Records Checks every two years for all airport and airline employee badge holders until an automated recurrent vetting solution is identified and in place; reinforcement of existing requirements that employees traveling as passengers be screened by TSA; reduction in the number of access points to secured areas; increase in random screening of employees; and implementation of a joint effort with our stakeholder partners to leverage the DHS "If You See Something, Say Something™" initiative to encourage reporting of insider threat activity. A few highlights of our progress include:

- TSA increased the number of employee screenings from 2.1 million in 2014 to 12.9 million in 2015 over a similar time period.
- Eighty-eight percent of U.S. airports have reduced the number of access points, resulting in an elimination of nearly 500 access points nationwide. TSA is continuing to pursue this initiative.
- TSA's Insider Threat Unit in the Office of Law Enforcement is closely collaborating with Federal and state partners to monitor criminal activity in airports. These actions have led to recent arrests in San Francisco, Dallas, Los Angeles, and Puerto Rico, and demonstrate a renewal of our efforts in this important mission area.

Additionally, TSA continues to implement the recommendations provided by the Aviation Security Advisory Committee (ASAC) on access control and perimeter security at airports nationwide. At the Secretary's request, the Aviation Security Advisory Committee provided TSA with 28 recommendations to reduce vulnerabilities against an insider threat. Consulting with the ASAC was an extremely productive approach to addressing access control vulnerabilities as their membership, drawn from industry, law enforcement, and other key stakeholders, brought a broad range of perspectives to the problem of insider threat and access control. On April 8, 2015, the ASAC provided its report to TSA, which addressed five security lines of effort:

- Security Screening and Inspection;
- Vetting of Employees and Security Threat Assessments;
- Internal Controls and Auditing of Airport-Issued Credentials;
- Risk-Based Security for Higher Risk Populations and Intelligence; and
- Security Awareness and Vigilance.

TSA appreciates the ASAC's timely and thoughtful review. TSA has implemented 10 of the ASAC report's 28 recommendations and continues to pursue implementation of the outstanding recommendations.

Vetting and Credentialing of Aviation Workers

Pursuant to statutory authority and regulations, TSA requires airport and airline employees to successfully complete a security threat assessment prior to receiving airport identification (ID) media granting access to non-public areas of the airport.

When individuals apply for employment with the airport or airline, they provide biographic and biometric data information that is used to conduct various security checks. TSA continuously runs the biographic information against the Terrorist Screening Database (TSDB), ensuring there are no ties to terrorism when the individual first applies for ID media and throughout the term of his or her employment at the airport. Also, TSA verifies that all individuals applying for airport ID media have lawful presence in the United States. Individuals who need access to the secure and sterile areas of the airport must also complete a criminal history records check to ensure that they have not committed a disqualifying offense listed in statute within the preceding 10 years. If the applicant successfully completes each phase of the security threat assessment, the airport may issue ID media. Based on security threat assessments, TSA estimates that there are approximately 1.6 million workers with access to SIDA, 1.4 million workers with access to the Sterile Area, and 1.2 million workers with access to Air Operations Area (AOA), noting that an individual worker may be granted access to more than one area with a properly coded badge.

TSA recognizes the value of conducting more frequent, or recurrent, criminal checks on workers to identify cases where there has been subsequent criminal activity since the original application. To date, TSA has been limited in its effort to implement this change because it is not considered a criminal justice agency and does not have access to recurrent criminal checks as are available to law enforcement agencies.

Nevertheless, TSA has pursued other options to gain this capability in a cost-effective manner. In September 2014, the FBI implemented a new automated capability called “Rap Back” that will provide criminal history monitoring services to both criminal justice and non-criminal justice agencies, such as TSA, for a reduced fee. TSA and the FBI are planning to pilot

Rap Back at Dallas/Fort Worth International Airport, Boston Logan International Airport, and at other airports in partnership with Delta Air Lines. The pilot program will provide employers real-time recurrent information on criminal activity committed by credential-holding employees. TSA also recognizes the value of having automated access to additional intelligence-related data in the Terrorist Identities Datamart Environment (TIDE) that may help to further inform TSA's vetting decisions. While TSA can already use this information in manual reviews of SIDA applicants, automated access will contribute to a more efficient STA process and allow TSA to assist the intelligence and law enforcement community based on the findings from the rest of its security threat assessment. TSA, working closely with the Department of Homeland Security and interagency partners, has requested and received approval for this automated access for additional information. This addresses a key Office of Inspector General recommendation. TSA is currently working on the necessary technical changes and policy notifications needed to support implementation and expects to begin receiving automated access to the majority of this data in the coming weeks.

Development and Execution of Security Plans

While TSA is responsible for conducting the vetting of aviation workers, airport operators are responsible for issuing and managing the ID media that allow individuals to have physical access to secure or sterile areas of the airport. TSA has established security program requirements, based on authorities found in Federal regulations, which airports are responsible to implement and follow. TSA maintains regulatory oversight of airports and conducts inspections to ensure the requirements are being followed. The Code of Federal Regulations, 49 CFR 1542.211 establishes the requirements for an airport authority, describes when they must issue

ID media, how they must account for that ID media, and, in combination with 49 CFR 1542.207, describes the security systems, policies, and procedures that are associated with the ID media, such as reporting lost or stolen ID media, retrieving and deactivating inactive/expired ID media, ensuring appropriate controls on the issuance of ID media, and conducting appropriate audits of the ID media process.

As described above, each airport operator is responsible for both issuing and controlling airport-issued credentials granting access to non-public areas of the airport. These responsibilities are decentralized to each airport, and the number of credentials and the technologies employed for badge recognition at each airport varies. This arrangement allows each airport operator to adjust its security plans for circulation control, consistent with local requirements. It also creates a credentialing enterprise that is more difficult and complex to defeat because of the variety of unique local systems, procedures, and requirements.

Inspections, Assessments, and Testing of Access Control Systems

TSA's authority to conduct inspections, assessments, and audits of airport access control plans provide a valuable enterprise-wide capability to enforce standards and drive security advancements. TSA requires that airport operators conduct recurring, comprehensive audits of all airport issued ID media and maintain records of those audits for one year, subject to TSA inspection. Individuals granted unescorted accesses are responsible for reporting lost or stolen ID media, and the airport ID systems and procedures must be capable of immediately denying access to any ID media reported lost or stolen. If the percentage of unaccounted for or lost ID media reaches an established threshold for a particular category of access, the airport must reissue all badges in that access category.

The Compliance Division within my office recently conducted a case review of badge audits for Fiscal Years 2010 through 2015. As part of that review, TSA concluded that only 23 of the nearly 440 federalized airports had exceeded the threshold over this five-year period, and therefore, were required to reissue badges. In addition, in June 2015, the Compliance Division completed a Special Emphasis Inspection of all federalized airports and concluded that the average percentage of unaccounted badges was significantly less than the threshold.

TSA also requires airport operators to implement provisions for controlling entry to non-public areas of the airport, and provide for detection of and response to unauthorized presence or movement in the controlled area. Aircraft operators are further required to prevent unauthorized access to their aircraft. TSA's enforcement mechanisms provide for a range of measures, from collaborating with stakeholders to address corrective actions for violations found during inspections to enforcement actions that include fines.

In 2013, TSA launched the Compliance Security Enhancement Through Testing (COMSETT) initiative to improve TSA and industry collaboration and promote more effective security, including airport access control. COMSETT is a data-driven process based on real-world outcomes of security system tests that reveal insights about vulnerability in near real time at both the local and national level. The COMSETT approach allows regulated entities to be tested initially without regulatory enforcement action, collaborate on best practices, and then retest to ensure compliance. Since the launch of COMSETT, TSA has seen improvements in overall compliance, and the agency continues to deploy these tests to address ongoing or any new vulnerabilities identified.

TSA has undertaken additional improvements in tightening airport access control, through its partnership with the FBI to conduct Joint Vulnerability Assessments (JVAs) of

airports. These comprehensive threat and vulnerability assessments are accomplished from an adversary's point of view, with the primary focus on identifying vulnerabilities that extend beyond Federal Regulation compliance and that may directly impact the aviation domain. At the conclusion of the JVA, TSA presents a final comprehensive report to the airport Federal Security Director (FSD) to be shared with pertinent airport stakeholders as an additional capability in our effort to reduce risk and improve an airport's security posture.

Random Screening of Aviation Workers

In addition to vetting and regulatory measures set in place, Transportation Security Officers and airport authority resources are deployed at random to screen airport and airline workers throughout the work day.

Specific TSA screening measures vary by time, location, and method to enhance unpredictability. Measures include ID verifications and searches of individuals and/or their property to detect and deter the introduction of prohibited items. Furthermore, airport operators are required to conduct random inspections of employees entering secure or sterile areas, to include ID verification and checks for prohibited items. If employees fail to follow proper procedures in accessing secure areas, they may be restricted from future access, disciplined by their employer, or subjected to criminal charges and civil penalties.

Conclusion

Thank you for the opportunity to appear before you today to discuss TSA's capabilities and risk-based approach to mitigating insider threat, including aviation worker credentialing. TSA will continue to apply risk-based, intelligence-driven security measures to address

vulnerabilities associated with employees who have access to aircraft and secure areas of the airport, and continue to work with industry representatives and the public to strengthen aviation security. I appreciate your interest in this issue and look forward to answering your questions.

Mr. MICA. Thank you so much.
 We'll go now to the inspector general, Mr. Roth.
 You're welcome and recognized.

STATEMENT OF JOHN ROTH

Mr. ROTH. Chairman Mica, Ranking Member Duckworth, and members of the subcommittee, thank you for inviting me here this afternoon to testify.

Since 2004, we have published more than 120 audit and inspection reports about TSA's programs and operations. Our work includes evaluations of passenger and baggage screening, TSA PreCheck, acquisitions, equipment deployment, and maintenance. We have also used covert testing to determine whether unauthorized and potentially dangerous individuals and items could gain access to secure airport areas.

The audit I am discussing this afternoon looked at how well TSA vets airport workers who have unrestricted access to secure areas of the airport. While we found that TSA's efforts to screen against the terrorist watch list were generally effective, we found that TSA did not have access to the complete terror watch list, known as the TIDE database. As a result, we identified 73 airport workers contained within that database who had been cleared to work in sensitive areas.

TSA officials recognize that not receiving the full database represents a weakness in its program and informed us that TSA could not guarantee that it can consistently identify all questionable individuals without receiving these categories. Fortunately, at the request of DHS, the National Counterterrorism Center, working as part of the interagency process, has changed their policy as a result of this audit, and TSA now or will soon have access to this information.

TSA is considerably challenged, however, when it comes to verifying workers' criminal histories and immigration status. First, TSA does not currently vet airport workers' criminal histories after they are initially cleared to work, but rely on individuals to self-report disqualifying crimes. As a result, individuals could lose their job if they report these crimes, so they have little incentive to do so.

Under the law, the 450 commercial airports maintain the ultimate authority to review and determine whether an individual's criminal history contains disqualifying crimes under Federal law. TSA officials informed us that airport officials rarely or almost never document the results of their reviews electronically. Thus, TSA cannot systematically determine whether individuals have been convicted of disqualifying crimes.

Instead, TSA performs annual manual inspections of commercial airport security operations, including the review of documents that aviation workers have submitted when applying for credentials. However, due to the large workload involved, particularly at larger airports, this inspection process looked at as few as 1 percent of all aviation workers' applications.

We also found weaknesses in the verification process for an individual's authorization to work in the United States. Airport operators are required to ensure that aviation workers are authorized to

work in the United States before they send their information to TSA for review. However, our review of TSA data showed that TSA has denied credentials to over 4,800 people because they could not show their lawful status to work. This occurred even after or even despite the fact that these individuals had been previously cleared by the airports as being authorized to work in the United States.

Lastly, the records TSA uses for vetting individuals is not reliable, as it contains incomplete or inaccurate data. For example, we found that there were 87,000 active aviation workers who did not have Social Security numbers listed, even though Social Security numbers are the best way to match individuals to existing records.

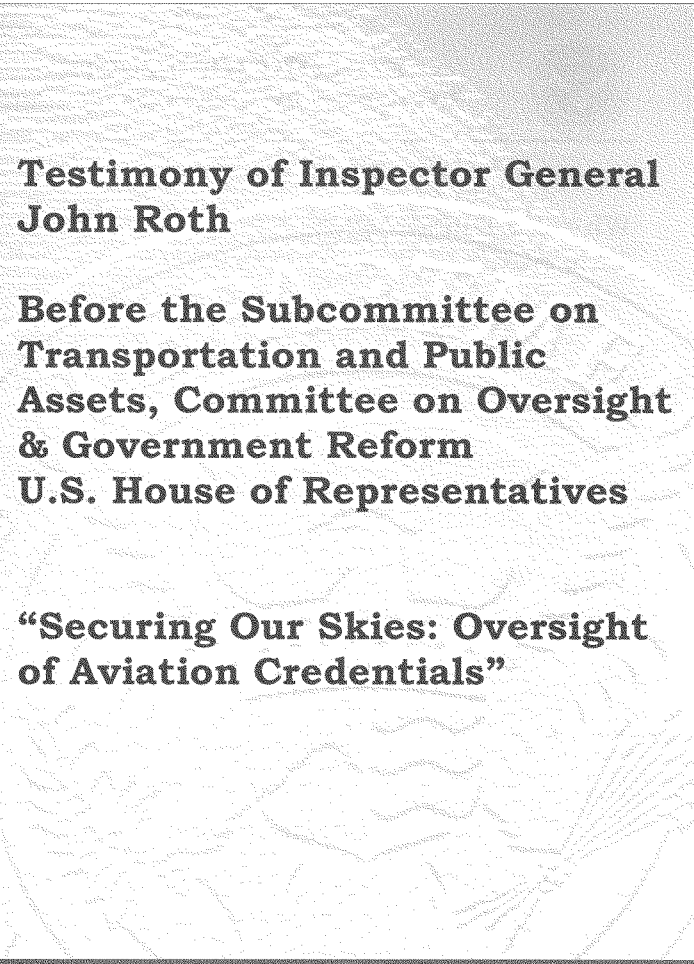
An additional 75,000 records listed individuals with active aviation worker credentials as citizens of non-U.S. countries, but did not include passport numbers. Of those records, over 14,000 individuals also did not list alien registration numbers.

TSA did not have appropriate checks in place to reject such records from vetting. Without complete and accurate information, TSA risked credentialing and providing unescorted access to secure airport areas for a worker who could potentially harm the Nation's air transportation system.

We made six recommendations in our report. TSA has agreed with all of our recommendations and has provided target completion dates for corrective action. We are satisfied with TSA's corrective actions to date, but we will continue to follow up on implementation of these actions.

Mr. Chairman, thanks again for inviting me here to testify. I look forward to discussing your work with you and other members of the subcommittee.

[Prepared statement of Mr. Roth follows:]



OFFICE OF INSPECTOR GENERAL

**Testimony of Inspector General
John Roth**

**Before the Subcommittee on
Transportation and Public
Assets, Committee on Oversight
& Government Reform
U.S. House of Representatives**

**“Securing Our Skies: Oversight
of Aviation Credentials”**



Homeland
Security

**February 3, 2016
1:00 PM**



DHS OIG HIGHLIGHTS

Securing Our Skies: Oversight of Aviation Credentials

February 3, 2016

Why We Did This Audit

We conducted this review to identify enhancements to the Transportation Security Administration's (TSA) vetting of workers with access to secure areas of commercial airports for links to terrorism, criminal history, and lawful status. We also assessed the accuracy and reliability of data TSA uses for vetting.

What We Recommend

TSA should request and review additional watchlist data, require that airports improve verification of applicants' right to work, revoke credentials when the right to work expires, and improve the quality of vetting data.

For Further Information:
Contact our Office of Legislative Affairs at (202) 254-4100, or email us at DHS-OIG-OfficeLegislativeAffairs@oig.dhs.gov

What We Found

TSA's multi-layered process to vet aviation workers for potential links to terrorism was generally effective. In addition to initially vetting every application for new credentials, TSA recurrently vetted aviation workers with access to secured areas of commercial airports every time the Consolidated Terrorist Watchlist was updated. However, our testing showed that TSA did not identify 73 individuals with terrorism-related category codes because TSA was not authorized to receive all terrorism-related information under the interagency watchlisting policy effective at the time of our audit.

TSA had less effective controls in place for ensuring that aviation workers 1) had not committed crimes that would disqualify them from having unescorted access to secure airport areas, and 2) had lawful status and were authorized to work in the United States. In general, TSA relied on airport operators to perform criminal history and work authorization checks, but had limited oversight over these commercial entities. Thus, TSA lacked assurance that it properly vetted all credential applicants.

Further, thousands of records used for vetting workers contained potentially incomplete or inaccurate data, such as an initial for a first name and missing social security numbers. TSA did not have appropriate edit checks in place to reject such records from vetting. Without complete and accurate information, TSA risks credentialing and providing unescorted access to secure airport areas for workers with potential to harm the nation's air transportation system.

TSA Response

TSA concurred with all six recommendations. As of the date of this testimony, three recommendations are closed and three are open and resolved, meaning that TSA and OIG have agreed on the corrective actions that TSA will take to close the recommendations.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Chairman Mica, Ranking Member Duckworth, and Members of the Subcommittee: thank you for inviting me here this afternoon to discuss the results of the Office of Inspector General's audit of the Transportation Security Administration's vetting of employees with access to secure areas of the airports.¹ We also reported on TSA worker vetting operations in 2011 and prior years.² In addition to reviewing vetting operations, in the past we have also used covert testing to determine whether unauthorized and potentially dangerous individuals could gain access to secured airport areas.³

TSA uses multiple layers of security to ensure the safety of the traveling public and transportation systems. Aviation worker vetting is just one area that we have reviewed; we have testified before this and other committees several times in the last year on multiple transportation security vulnerabilities that we believe TSA needs to address. Since 2004, we have published more than 120 audit and inspection reports about TSA's programs and operations. Our work includes evaluations of passenger and baggage screening, TSA PreCheck, TSA acquisitions, and TSA equipment deployment and maintenance.

In our most recent audit on aviation worker vetting, we generally found:

- TSA's layered controls for vetting workers for terrorism are generally effective. However, TSA did not identify 73 individuals with terrorism-related category codes because it was not authorized to receive all terrorism-related categories under current interagency watchlisting policy.
- TSA had less effective controls in place to ensure that airports have a robust verification process over a credential applicant's criminal history and authorization to work in the United States.
- TSA needs to improve the quality of data used for vetting purposes.

My testimony today will discuss each of these areas in further detail.

BACKGROUND ON TSA VETTING

TSA was created in 2001 to ensure the safety and free movement of people and commerce within the Nation's transportation systems. As part of this mission,

¹ *TSA Can Improve Aviation Worker Vetting (Redacted)*, OIG-15-98

² *TSA's Oversight of the Airport Badging Process Needs Improvement*, OIG-11-95; *TSA Vetting of Airmen Certificates and General Aviation Airport Access and Security Procedures*, OIG-11-96; *Transportation Security Administration's Aviation Channeling Services Provider Project*, OIG-13-42; *TSA's Security Screening Procedures for Employees at Orlando International Airport and the Feasibility of 100 Percent Employee Screening*, OIG-09-05

³ *Covert Testing of Access Controls to Secured Airport Areas*, OIG-12-26



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

TSA has statutory responsibility for properly vetting aviation workers such as baggage handlers and airline and vendor employees.

Federal regulations require individuals who apply for credentials to work in secure areas of commercial airports to undergo background checks. TSA and airport operators are required to perform these checks prior to granting individuals badges that allow them unescorted access to secure areas. Each background check includes:

- a security threat assessment from TSA, including a terrorism check;
- a fingerprint-based criminal history records check (CHRC); and
- evidence of the applicants' authorization to work in the United States.

Airports collect the information used for vetting, including each applicant's name, address, date of birth, place of birth, country of citizenship, passport number, and alien registration number (if applicable). TSA also relies on airport or air carrier employees to collect applicants' fingerprints for the CHRC.

Once it receives biographic data, TSA electronically matches credential applicants against its extract of the Government's Consolidated Terrorist Watchlist to identify individuals with potential links to terrorism. TSA also recurrently vets airport workers every time it receives a watchlist update. TSA identifies potential matches to terrorism-related information using varied pieces of data such as name, address, Social Security number (SSN), passport number, and alien registration number. TSA analysts manually review potential matches to determine whether cases represent a true match of an applicant to terrorism-related information and the risk posed by the case. Based on this review, TSA may direct the airport to grant, deny, or revoke a credential after coordination with other governmental organizations.

Airport operators are responsible for reviewing aviation worker criminal histories and his/her authorization to work in the United States. For the criminal history check, applicants submit fingerprint records through airport operators and TSA for transmittal to the FBI. TSA then receives the results of the fingerprint check and provides them to airport operators for review. Certain criminal offenses—such as espionage, terrorism, and some violent offenses and felonies—are disqualifying offenses that should prevent an individual from unescorted access to secured areas of an airport. TSA and the airports also conduct checks to verify an individual's immigration status and authorization to work, respectively.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

RESULTS

Vetting for Terrorism Links

We found that TSA was generally effective in identifying individuals with links to terrorism. Since its inception in 2003, TSA has directed airports to deny or revoke 58 airport badges as a result of its vetting process for credential applicants and existing credential holders. In addition, TSA has implemented quality review processes for its scoring model, and has taken proactive steps based on non-obvious links to identify new terrorism suspects that it nominates to the watchlist.

Despite rigorous processes, TSA did not identify 73 individuals with links to terrorism because TSA is not cleared to receive all terrorism categories under current inter-agency watchlisting guidance.⁴ At our request, the National Counterterrorism Center (NCTC) performed a data match of over 900,000 airport workers with access to secure areas against the NCTC's Terrorist Identities Datamart Environment (TIDE). As a result of this match, we identified 73 individuals with terrorism-related category codes who also had active credentials. According to TSA officials at the time of our report, current interagency policy prevented the agency from receiving all terrorism-related codes during vetting.

TSA officials recognized that not receiving these codes represents a weakness in its program, and informed us that TSA cannot guarantee that it can consistently identify all questionable individuals without receiving these categories. In 2014, the TSA Administrator authorized his staff to request some missing category codes for vetting. However, according to an official at the DHS Office of Policy, TSA needed to work with DHS to formalize a request to the Watchlisting Interagency Policy Committee in order to receive additional categories of terrorism-related records. Recently, TSA informed us that it has taken actions to address this issue. Since the issuance of our report, we have received documentation satisfying our office that TSA has taken corrective action to address this weakness.

Vetting for Criminal Histories

Airport operators review criminal histories for new applicants for badges to secure airport areas after receiving the results of FBI fingerprint checks through TSA but do not conduct recurrent criminal history vetting, except for the U.S. Marshals Service Wants and Warrants database. This is because

⁴ The Interagency Policy Committee responsible for watchlist policy determines what terrorism-related categories are provided to TSA for vetting, while the DHS Watchlist Service provides allowable information to TSA.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

aviation worker vetting is considered to be for non-criminal justice purposes. Instead, we found airports relied on individuals to self-report disqualifying crimes. As individuals could lose their job if they report the crimes, individuals had little incentive to do so.

TSA also did not have an adequate monitoring process in place to ensure that airport operators properly adjudicated credential applicants' criminal histories. While TSA facilitated the CHRC for aviation worker applicants, over 400 commercial airports maintained the ultimate authority to review and determine whether an individual's criminal history contained disqualifying crimes under Federal law. TSA officials informed us that airport officials rarely or almost never documented the results of their CHRC reviews electronically. Without sufficient documentation, TSA cannot systematically determine whether individuals with access to secured areas of the airports are free of disqualifying criminal events.

TSA has taken steps to address weaknesses in criminal history vetting. TSA has planned a pilot of the FBI's "Rap Back" program to receive automated updates from the FBI for new criminal history matches associated with airport workers so that the airports can take actions. Recently, TSA informed us that it plans to start this pilot program for multiple airports in February 2016.

Vetting for Authorizations to Work

We also found weaknesses in the verification process for an individual's authorization to work in the United States. Airport operators are required to ensure that aviation workers are authorized to work in the United States prior to sending their information to TSA for review. TSA then verifies that aviation workers have lawful status to be in the United States. However, our review of TSA data showed that TSA has had to send nearly 29,000 inquiries to credential applicants regarding their lawful status since program inception in 2004. Of those individuals, over 4,800 were eventually denied credentials because TSA determined that they did not prove lawful status even after appeal. This occurred despite the fact that these individuals had previously received clearance from the airports as being authorized to work.

Additionally, we found that TSA did not require airports to restrict the credentials of individuals who may only be able to work in the United States temporarily. Consequently, airports did not put expiration dates on the badges. Although airports are required to verify work authorizations upon badge renewal every 2 years, or whenever another credential is requested, individuals may continue to work even when they no longer have lawful status during the period between badge renewals. Without ensuring that an individual's credential is voided when he or she is no longer authorized to work, TSA runs



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

the risk of providing individuals access to secure airport areas even though they no longer have the authorization to work in the United States.

TSA's Office of Security Operations performed annual inspections of commercial airport security operations, including reviews of the documentation that aviation workers submitted when applying for credentials. However, due to workload at larger airports, this inspection process looked at as few as one percent of all aviation workers' applications. In addition, inspectors were generally given airport badging office files, which contained photocopies of aviation worker documents rather than the physical documents themselves. An official from this office told us that a duplicate of a document could hinder an inspector's ability to determine whether a document is real or fake, because a photocopy may not be matched to a face, and may not show the security elements contained in the identification document. Fortunately, as a result of our audit, TSA has taken corrective action and TSA inspectors will now be able to examine original documents during annual security inspections.

TSA Can Improve the Reliability of Its Vetting Data

TSA relied on airports to submit complete and accurate aviation worker application data for vetting. However, we identified thousands of aviation worker records that appeared to have incomplete or inaccurate biographic information as follows:

- 87,000 active aviation workers did not have SSNs listed even though TSA's data matching model identified SSNs as a strong matching element.
- 1,500 records in TSA's screening gateway had individuals' first names containing two or fewer characters.
- Over 300 name records contained a single character.
- An additional 75,000 records listed individuals with active aviation worker credentials as citizens of non-U.S. countries, but did not include passport numbers. Out of those records, over 14,000 also did not list alien registration numbers. According to TSA, the passport number is a desired field to collect, but is not required.

In addition to the data completeness issues that we identified, TSA independently determined that airports may not be providing all aliases used by applicants undergoing security threat assessments. This typically occurred when TSA's vetting process discovered that individuals had used aliases. Complete and accurate aliases are important to the accuracy and effectiveness of TSA's vetting processes. TSA has directed airports to report all aliases; however, to the extent that airports do not ensure that aliases are captured



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

and provided to TSA, TSA terrorism vetting may be limited for certain individuals.

TSA has taken steps to address some of these weaknesses. TSA made system enhancements between 2012 and 2014 designed to improve the quality of data that it received from airports. For example, TSA will refuse to vet individuals if their birthdates show that they are younger than 14 or older than 105 and encourage airports to submit electronic copies of immigration paperwork with applications to expedite the vetting process. These enhancements were expected to become effective for new or reissued badges within 2 years of being implemented. Recently, TSA informed us that it has drafted additional data requirements that will become effective in the second quarter of FY 2016.

CURRENT STATUS OF RECOMMENDATIONS

We made six recommendations in our report. TSA agreed with all of our recommendations and provided target completion dates for corrective actions. To date, TSA has completed corrective actions to close three of our recommendations, and has reported actions underway to close the remaining three recommendations in the second quarter of FY 2016. TSA considers many details of its corrective actions to be Sensitive Security Information and we cannot include them here. In addition, TSA has performed its own review of the 73 individuals we identified with terrorism-related category codes and determined that none of the individuals represented a threat to transportation security. However, TSA's inability to have access to all terrorism-related information presents a risk to transportation security, and we are pleased that TSA has taken corrective actions in response to our audit recommendation that address that risk. Following is the current status of our six recommendations.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Table 1: Status of OIG Recommendations to Enhance TSA's Vetting of Aviation Workers

Recommendation	Current Status	Details
Follow up on the request for additional categories of terrorism-related records	CLOSED	Closed in January 2016. TSA considers details of its corrective actions to address this recommendation to be Sensitive Security Information.
Require inspectors to view original identity documents supporting airport adjudication of an applicant's criminal history and work authorization	CLOSED	TSA provided documentation in October 2015 that it had updated its Compliance Program Manual for Transportation Security Inspectors to comply with our recommendation.
Pilot FBI's Rap Back Program and take steps to institute recurrent vetting of criminal histories at all commercial airports	OPEN, RESOLVED	TSA reported in January 2016 that it projected the pilot program to begin in February 2016.
Require airports to link credential end dates to temporary work authorization end dates	CLOSED	TSA provided documentation in December 2015 to show it had posted additional guidance for airport operators to deactivate badges promptly when an individual's authorization to work ends.
Perform analysis to identify and address airports' weaknesses in determining applicants' lawful status	OPEN, RESOLVED	TSA reported in January 2016 that it was reviewing records and anticipated closure in the second quarter of FY 2016.
Implement data quality checks to ensure complete and accurate data as required by TSA policy	OPEN, RESOLVED	TSA reported in January 2016 that it had identified enhancements and anticipated closure in the second quarter of FY 2016.

Our office will continue to follow up on implementation of these corrective actions.

ONGOING REVIEWS

We have two additional ongoing reviews related to the TSA credentialing process. First, we are reviewing TSA's oversight of airport operators' accountability procedures for Secure Identification Display Area (SIDA) badges, which airport operators issue to airport and TSA employees who require access to secure areas. TSA oversees the implementation of airport operators' security programs, including the accountability procedures for SIDA badges and access



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

control systems. We are testing selected internal controls airport operators have in place to mitigate the potential risks of unaccounted for, lost, or stolen SIDA badges. OIG has tested selected internal controls at 24 of the largest U.S. airports and will issue a report on our findings later this year.

We are also reviewing the applicant screening process for Transportation Workers Identification Credential (TWIC) program to determine whether it is operating effectively and ensuring only eligible TWIC card holders remain in the program. We expect to complete this review this summer, but because of some of our preliminary findings, TSA has already begun assessing some program shortfalls.

CONCLUSION

TSA has the responsibility to ensure transportation security and the free and safe movement of people and commerce throughout the Nation. Effectively carrying out this responsibility is of paramount importance, given emerging threats and the complex and dynamic nature of this Nation's transportation system. We previously testified about major TSA deficiencies in accomplishing its transportation security mission, including extensive failures at TSA checkpoints identified during recent penetration testing, as well as weaknesses in its PreCheck vetting and screening process. With our recent report, we add another security vulnerability that TSA must address: ensuring it has all relevant terrorism-related information when it vets airport employees for access to secure airport areas. We will continue to monitor TSA's progress as it takes corrective actions to address these vulnerabilities.

COMPUTER MATCHING ACT EXCEPTION

I would be remiss if I did not mention the data matching issues that we encountered while conducting this audit. As part of this review, we collaborated with the NCTC to perform a data match of aviation worker's biographic data against TIDE to determine if TSA identified all individuals with potential links to terrorism. Because we do not have an exemption from the Computer Matching Act, it took us 18 months to get a Memorandum of Understanding in place with the NCTC in order to perform this data match – and that was with full cooperation from the NCTC.

We support pending legislation co-sponsored by the Chairman and Ranking Member of the full Committee, the *Inspector General Empowerment Act* (H.R. 2395), that would give Inspectors General a computer matching exception. This would enable us to conduct these types of audits on a more frequent basis and with greater ease. We are grateful that the legislation has been reported to the House by this Committee and are hopeful for continued legislative action this Congress.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Mr. Chairman, thank you for inviting me to testify here today. I look forward to discussing our work with you and the Members of the Subcommittee.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix A
Reports Cited in Testimony

TSA Can Improve Aviation Worker Vetting (Redacted), OIG-15-98 (June 2015)

Transportation Security Administration's Aviation Channeling Services Provider Project, OIG-13-42 (February 2013)

TSA's Oversight of the Airport Badging Process Needs Improvement, OIG-11-95 (July 2011)

TSA Vetting of Airmen Certificates and General Aviation Airport Access and Security Procedures, OIG-11-96 (July 2011)

Covert Testing of Access Controls to Secured Airport Areas, OIG-12-26 (January 2012)

TSA's Security Screening Procedures for Employees at Orlando International Airport and the Feasibility of 100 Percent Employee Screening, (OIG-09-05) (October 2008)



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
Current and Planned OIG Work on TSA

Projects In-Progress:

Project Topic	Objective
TSA Security Vetting of Passenger Rail Reservation Systems	Determine the extent to which TSA has policies, processes, and oversight measures to improve AMTRAK security.
Reliability of TWIC Background Check Process	Determine whether the screening process for the TWIC program is operating effectively and whether the program's processes ensure that only eligible TWIC card holders remain in the program.
TSA's Security Technology Integrated Program (STIP)	Determine whether TSA has incorporated adequate IT security controls for passenger and baggage screening STIP equipment to ensure it is performing as required.
TSA's Controls Over Access Media Badges	Identify and test selected controls over access media badges issued by airport operators.
TSA's Risk-Based Strategy	Determine the extent to which TSA's intelligence-driven, risk-based strategy informs security and resource decisions.
Airport Security Capping Report	Synthesize the results of our airport security evaluations into a capping report that recommends how TSA can systematically and proactively address these issues at airports nationwide.

Upcoming Projects:

Project Topic	Objective
Federal Air Marshal Service's Oversight of Civil Aviation Security	Determine whether the Federal Air Marshal Service adequately manages its resources to detect, deter, and defeat threats to the civil aviation system.
TSA Carry-On Baggage Penetration Testing	Determine the effectiveness of TSA's carry-on baggage screening technologies and checkpoint screener performance in identifying and resolving potential security threats at airport security checkpoints.
TSA's Classification Program	Determine whether TSA is effectively managing its classification program and its use of the Sensitive Security Information designation.
TSA's Office of Intelligence and Analysis	Determine whether TSA's Office of Intelligence and Analysis is effectively meeting its mission mandates.
Verification Review – TSA's Screening of Passengers by Observation Techniques	Conduct a verification review to ensure TSA has implemented our closed recommendations from our September 2013 report.

Mr. MICA. Thank you.
 We will recognize FAA representative Margaret Gilligan.
 Welcome back, and you're recognized.

STATEMENT OF MARGARET GILLIGAN

Ms. GILLIGAN. Thank you, Chairman Mica. Thank you, Ranking Member Duckworth and members of the subcommittee. I welcome this opportunity to appear before you today on the issue of oversight of aviation credentials. I know this is an issue of significant interest to Chairman Mica because we have appeared on this issue under your leadership before, sir.

The mission of the FAA is ensuring the highest levels of safety for the millions of passengers flying every day. The agency is charged with the oversight of airlines and aircraft manufacturers, the safety of our Nation's airports, and training our air traffic controllers. Taken together, we operate the safest and most efficient airspace system in the world.

The FAA issues 23 different types of airman certificates, including those to pilots, mechanics, dispatchers, flight attendants, and air traffic controllers. There are more than 800,000 active pilot certificate holders alone.

A pilot certificate is a credential attesting to the training and competence of the pilot. It is the same as a lawyer who must have evidence of admission to the bar or a doctor who is board certified in a specialty.

In all these cases, the credential is not used as identification media, and it does not impart security access to courtrooms, to operating rooms, or to airports. A pilot never uses his or her pilot certificate to gain access to airport areas. Instead, he or she uses the security credential issued by the airport, as required by TSA.

Since 2002, FAA has taken actions to enhance the security of pilot certificates. We require pilots to carry a valid government-issued photo ID in addition to a pilot certificate whenever they're flying. This allows an FAA inspector or others to confirm both the pilot's identity and his or her pilot qualification.

The FAA phased out paper certificates and incorporated tamper- and counterfeit-resistant features, including microprinting, a hologram, and a UV-sensitive layer. In 2010, FAA issued a notice of proposed rulemaking to require a photo on pilot certificates and to improve the process for getting a student pilot certificate.

While we were preparing that final rule, the FAA Modernization and Reform Act required that the pilot certificate accommodate fingerprints, iris, and comply with specific security standards. Unfortunately, our 2010 proposal did not include those security requirements, and to allow the pilot community as well as the general public to comment on the full statutory mandate, we needed to draft a new proposal.

However, at the same time, the security and intelligence communities determined that allowing student pilots to operate an aircraft as pilot in command prior to being vetted was an unacceptable security risk. The administration committed to closing that security gap, and last month, FAA published a final rule requiring student pilots to appear before an FAA inspector or other author-

ized designee to verify the student's identity. The student pilot certificate will be issued once TSA completes its vetting.

We recognize that the 2012 legislation included specific direction on airman certificates, and we regret that we are not further along in the process of implementing those provisions. But as our 2013 report to Congress outlined, there are major challenges to implementing the congressional direction. While the National Institute for Standards and Technology has issued standards for the collection of iris images, there are no approved GSA products—there are no GSA-approved products for the collection or use of iris biometrics.

Before we require collection of biometrics, we need to understand where and how they would be used. There are no requirements that airports use iris or other biometric information for authorizing access at airports. So neither FAA nor TSA have estimated the costs to develop and install such an infrastructure at nearly 550 airports eligible for Federal grant funds or the more than 5,000 airports that are open to the public. As part of our rule to require biometrics, we will have to estimate what the costs of that infrastructure system will be to the airports and to the taxpayer.

In our report to Congress and in the preliminary work we have done on the rule, we estimated that the new certificates will cost more than a billion dollars over 12 years. As both Congress and the administration are committed to minimizing the costs to the public of Federal actions, that cost estimate alone may be our biggest challenge. The reality is that to include biometric information on pilot certificates drives costs and may not be the most effective way to meet our security objectives.

FAA has worked with TSA to develop options to accomplish the congressional direction. We will work to publish a proposal, although demonstrating benefits to justify a billion or more dollars in costs will be very difficult, and we will keep Congress informed on our progress.

That concludes my remarks, sir, and I'll be happy to answer any questions.

[Prepared statement of Ms. Gilligan follows:]

STATEMENT OF MARGARET GILLIGAN, ASSOCIATE ADMINISTRATOR FOR AVIATION SAFETY, FEDERAL AVIATION ADMINISTRATION, BEFORE THE HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM, SUBCOMMITTEE ON TRANSPORTATION AND PUBLIC ASSETS, ON "SECURING OUR SKIES: OVERSIGHT OF AVIATION CREDENTIALS," February 3, 2016.

Chairman Mica, Ranking Member Duckworth, Members of the Subcommittee:

Thank you for the opportunity to appear before you today on the issue of oversight of aviation credentials. I know that this issue has been and continues to be of significant interest to Chairman Mica. The Federal Aviation Administration (FAA) previously appeared on this issue before the Subcommittee on Government Operations in 2013 and before the Committee on Transportation and Infrastructure in 2011, both under Chairman Mica's leadership.

FAA continues to support the Transportation Security Administration (TSA) and other security and intelligence agencies to keep our skies secure. FAA is mindful of the risks identified by our security partners and has taken steps to close security gaps as advised by these agencies.

The FAA issues 23 different types of airman certificates, held by mechanics, dispatchers, parachute riggers, and air traffic controllers, in addition to the 6 types held by pilots. Active pilot certificate holders number approximately 861,000. Historically, a pilot certificate was evidence that the pilot was trained and competent to conduct the operations authorized by the certificate. The certificates, used for decades, worked effectively for this intended purpose.

As other agencies with mandates other than aviation safety began to see potential misuse of pilot certificates, FAA took steps to enhance the security of all airman certificates. Pursuant to the

Drug Enforcement Administration (DEA) Act of 1988, for example, the agency phased out paper certificates and replaced them with plastic certificates that incorporate tamper- and counterfeit-resistant features including micro printing, a hologram, and a UV-sensitive layer.

Since 2002, the FAA has required a pilot to carry a valid Government issued photo I.D. in addition to a pilot certificate while exercising the privileges associated with the certificate. This allows an FAA inspector, or a fixed base operator who rents airplanes, to confirm both the pilot's identity and his or her pilot qualifications.

Each time a pilot applies for a certificate or rating, the applicant is required to present an acceptable form of photo identification to the FAA inspector or designee. Acceptable forms of identification include a driver's license issued by a State, the District of Columbia, or a territory or possession of the United States; a Government issued identification card; or a passport. In addition to a photo, the identification must include the applicant's signature and residential address, if different from the applicant's mailing address. This information may be presented in more than one form of identification, and special procedures exist to verify the identity of applicants who do not possess suitable forms of identification, such as minors. We allow these alternatives because a pilot certificate does not impart security access privileges and the intended purpose of the certificate is not for use as an identification media or security credential, but simply to affirm a pilot's qualification.

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) imposed additional requirements for pilot certificates, including that they be tamper-resistant and include a photograph of the pilot. The certificates were also required to be capable of accommodating a

biometric identifier, such as a digital photo or fingerprint, or any other unique identifier FAA deemed necessary.

FAA met some of these requirements when it began issuing tamper- and counterfeit-resistant plastic certificates in 2003. In response to the remaining requirements of IRTPA, the FAA issued a Notice of Proposed Rulemaking (NPRM) in 2012 to require a photo of the pilot on all plastic pilot certificates, and student pilots to apply for, obtain, and carry plastic certificates while exercising the privileges of the student pilot certificate. While the agency was reviewing the hundreds of comments received on the NPRM, the FAA Modernization and Reform Act of 2012 became law. Section 321 of that Act required that pilot certificates not only contain photographs, but also be smart cards that can accommodate iris and fingerprint biometric identifiers and comply with FIPS-201 or Personal Identity Verification-Interoperability Standards (PIV-1) for processing through security checkpoints into airport sterile areas. The FAA's 2012 NPRM did not contemplate those additional features.

Upon further review of the NPRM, the security and intelligence communities identified a security gap in FAA's process for issuing student pilot certificates. With respect to this population, applicants could be issued a student pilot certificate before TSA had vetted the applicants. In 2012, the agency shifted its focus to closing the security gap in student pilot vetting. On January 12 of this year, the FAA published a final rule requiring student pilots to apply for a plastic certificate by appearing in person at a Flight Standards District Office (FSDO) or before a designated pilot examiner, an airman certificate representative associated with a flight school, or a certified flight instructor. These authorized individuals will be able to accept a student pilot application and verify the applicant's identity, but will not be able to issue a student

pilot certificate. The Civil Aviation Registry, located in Oklahoma City, Oklahoma, will provide the applicant's information to TSA for vetting before the certificate is issued. The Civil Aviation Registry will issue a permanent student pilot certificate only after receiving a positive response from TSA.

In 2013, we prepared and submitted a report to Congress on Section 321. As discussed in our report, an initial estimate of the cost of the transition to an enhanced pilot certificate is approximately \$1.125 billion over 12 years.

Given the substantial cost to pilots and taxpayers, we must coordinate with the Department of Homeland Security (DHS) and TSA to carefully consider the benefits of enhanced pilot certificates. If pilot certificates with embedded biometrics are intended to permit airport access or increase security, hundreds of airport access control systems would have to be created or retrofitted to ensure consistent use and verification of the biometrics.

In this regard, the National Institute of Standards and Technology (NIST) has developed standards defining how to collect iris biometric data. Now other government agencies, however, will need to develop the infrastructure to utilize this information. Understanding how best to use biometric data to enhance the security of the pilot community and aviation security overall will require continued coordination among government agencies in cooperation with airlines, airports, aviation labor groups, and others. FAA must also be mindful of the costs and benefits of these security enhancements as it evaluates the feasibility of a rule that can meet statutory mandates and accommodate rapidly evolving technologies.

Mr. MICA. Thank you. And we'll hold the questions.
 Let's get to Ms. Carroll, who's vice president of HID Global.
 Welcome, and you're recognized.

STATEMENT OF KATHLEEN M. CARROLL

Ms. CARROLL. Good afternoon, Chairman Mica and Ranking Member Duckworth. Thank you for the opportunity to appear before you today to discuss how private industry can contribute to and support all stakeholders in securing our Nation's airports.

I am testifying on behalf of the Security Industry Association, a nonprofit international trade association representing more than 600 companies. I am the chair of SIA's Government Relations Committee, and I also chair the Privacy and Public Policy Working Group at the IBIA.

We believe that to confront the ever-evolving threats to aviation security, all stakeholders should be working more closely with private industry. We recognize that TSA has been working diligently toward solutions that further enhance security in the Nation's airports. To that end, TSA requested that the Aviation Security Advisory Council analyze the adequacy of existing security measures and recommend additional measures to improve employee access controls.

One of those recommendations included biometric confirmation of identity for badge issuance. Biometrics are already in use at several airports across the Nation, including BWI and San Francisco. These biometric deployments enhance security by tying the badge to the holder of the badge. Biometric technology has improved substantially in recent years, and industry continues to invest in further advancements.

There are several key measures to help ensure optimum performance of a biometric system that should be included in any standard that TSA establishes. One is false acceptance rates, which sets the level of security. Another is the false rejection rate, which delivers a good customer experience. You can't have one without the other.

Another key measure is liveness detection, which eliminates spoofing. For example, liveness detections would solve the worry around the biometrics that were stolen during the OPM breach. Biometric information is worthless if it isn't usable. With liveness detection, the only way it is usable is if the living human being presents their biometrics.

Beyond biometrics, the security industry suggests that airport worker credentials follow a federated model. Many airport employees work at multiple airports and often need to go through the vetting process and carry a badge for each airport.

In a federated model, such as the U.S. Government's Personal Identity Verification program, each Federal employee is vetted to an acceptable and known process across all Federal agencies. PIV credentials use the Public Key Infrastructure as one of several security features so that the credential can be trusted for access to all government buildings and computer networks. PKI also allows for instant revocation of a credential across all these systems from a central location.

A federated credential system would significantly enhance airport security, be more convenient for airport employees, and reduce the costs of having to issue multiple credentials.

As the ASAC and TSA have recognized, the best security relies on a risk-based approach, and one that is layered so that a breach in any one layer does not compromise security. The use of CCTV cameras, physical access control systems, and physical barriers are just some of the layers in use at airports today.

The ASAC report also recommends an audit process that reconciles a badge holder's work schedule with the access control system to identify anomalies or irregularities, such as an employee using his or her badge at the airport outside their normal work hours. Unfortunately, this looks into the past and will not detect such anomalies in real time when a security breach might be occurring.

The security industry has developed identity management systems that serve as systems of record for every airport worker and will detect anomalies or deviations from normal work patterns in real time. These systems will alert airport security if anomalies deviations occur so they can be investigated immediately if necessary.

Equally important, such identity management systems, which are being used by several major airports throughout the country, are structured so that they enforce all TSA guidelines for badging and meet airport security policy as determined by each airport. These same systems can conduct audits recommended by the ASAC to ensure that an authorized signatory is in compliance with badging requirements.

In the future, as TSA explores the use of social media to track and assess emerging threats that may pose a risk to aviation, identity management systems could prove to be a valuable tool in automating this vital undertaking.

It's important to remember that the credential is just one piece of the security solution. The infrastructure must be in place to authenticate and authorize badge holders in an always-connected environment.

I want to thank the committee again for including the security industry in this important discussion. We welcome the opportunity to contribute to improve the aviation and airport security nationwide. I look forward to your questions.

[Prepared statement of Ms. Carroll follows:]

Testimony of Kathleen M. Carroll
Vice President, Government Affairs
HID Global
on behalf of the Security Industry Association (SIA)
before the
United States House of Representatives
Committee on Oversight and Government Reform
Subcommittee on Transportation and Public Assets
Securing Our Skies: Oversight of Aviation Credentials

February 3, 2016

Good afternoon Chairman Mica, Ranking Member Duckworth and distinguished Members of the Committee. Thank you for the opportunity to appear before you today to discuss how private industry can contribute to and support all stakeholders in securing our Nation's airports.

I am testifying on behalf of the Security Industry Association (SIA), a non-profit international trade association representing more than 600 companies that develop, manufacture and integrate electronic and physical security solutions. SIA member companies provide security solutions to the Department of Homeland Security and its components to help protect critical infrastructure, including chemical facilities, seaports, mass transit systems, government facilities, and the nation's airports. I am the Chair of SIA's Government Relations Committee and I also chair the Privacy and Public Policy Committee for the International Biometrics and Identification Association (IBIA).

The Security Industry Association's member companies recognize that TSA has built a multi-layered security system that is risk-based. It is our belief that to confront ever-evolving threats to aviation security, all stakeholders – airlines, airports, vendors, and government agencies – should be working more closely with private industry. We believe that if we work closely with all stakeholders, we can increase security exponentially.

We also recognize that TSA has been working diligently towards solutions that further enhance security in the nation's 440 airports. To that end, TSA requested that the Aviation Security Advisory Council (ASAC) analyze the adequacy of existing security measures and recommend additional measures to improve employee access controls.

For purposes of my testimony today, I am going to address those areas where SIA and its member companies are already providing security solutions that will help the TSA and all stakeholders better secure our nation's airports and ensure the safety of the traveling public.

The ASAC identified five areas of analysis and generated 28 recommendations where TSA and the airline industry can take action to address potential vulnerabilities. I will focus on just a few. First, I will comment on the recommendation for biometric confirmation of identity for badge issuance and random auditing capture of a biometric template of SIDA (a security identification display area badge) applicants.

Biometrics are already in use at several airports, including BWI and SFO. These biometric deployments enhance security by tying the SIDA badge to the holder of the badge. Further, biometric technology has improved substantially in recent years and industry continues to invest in further advancements. There are several key measures to help ensure optimum performance of a biometric system that should be included in any standard that TSA establishes as recommended by the ASAC.

One is false acceptance rate or FAR which sets the level of security. Another is the false rejection rate which delivers a good customer experience. You can't have one without the other. Another key measure is liveness detection which eliminates spoofing. For example, liveness detection solves the worry around the biometrics that were stolen in the OPM breach. Biometrics information is worthless if it isn't usable. With liveness detection, the only way it is usable is if the living human being presents their biometrics. The bottom line: biometrics uniquely identifies airport employees in a consistent and secure manner.

Beyond biometrics, the security industry recommends that airport worker credentials follow a federated model. Why? And what is a federated credential? Many airport employees work at multiple airports and often need to go through the vetting process and carry a badge for each airport. In a federated model, such as the US Government's Personal Identity Verification (PIV) program, each federal employee is vetted to an acceptable and known process across all Federal agencies.

This multiple credentialing requires that employees who cross-credential carry a variety of documents with them all the time – passport, driver's license, even social security cards and/or birth certificates. There is a tremendous security risk in carrying all of this critical and sensitive documentation all the time.

PIV credentials use the Public Key Infrastructure (PKI) as one of several security features so that the credential can be trusted for access to all physical government buildings and all computer networks. In addition, the PIV credential is built on the Federal Information Processing Standard created by NIST. And, PKI allows for instant revocation of a credential across all these systems from a central location. This satisfies the requirement that badges be deactivated when a worker is terminated.

Airports are like the Federal government. Employees from different airlines fly to multiple airports several times a day. Airline and airport employees have access to sensitive, sterile areas within the airport. And while some steps have been taken by some airports, the deficiency is that the solutions are all local. A federated credential system would significantly enhance airport security, be more convenient for airport employees and reduce the cost of having to issue multiple credentials.

Some airline crews carry a Known Crew Member credential that contains a barcode, but they also must present an employee ID card and a third credential such as a driver's license or passport to a TSA agent. Unfortunately for airport security, barcode technology is more appropriate for low-risk environments. This creates a significant security gap in that the TSA cannot be sure that the employee presenting the KCM card has not compromised the system. It is possible that someone could create a fraudulent KCM card, employee card and driver's license.

As the ASAC and TSA have recognized, the best security relies on a risk-based approach and one that is layered so that a breach in any one layer does not compromise security. The use of CCTV cameras, physical access control systems and physical barriers are just some of the layers in use at airports today.

The ASAC report also recommends a Work Schedule Audit to reconcile the badge holder's work schedule with the access control systems during a specified period to identify access anomalies or irregularities such as an employee using his or her badge at the airport outside of their normal work hours. Unfortunately, this looks into the past and will not detect such anomalies in real-time when a security breach might be occurring.

The security industry has developed identity management systems that serve as systems of record for every airport worker and will detect anomalies or deviations from normal work patterns in real time. These systems will alert airport security as anomalies/deviations occur so they can be investigated immediately if necessary.

Equally important, such identity management systems, which are being used by several major airports throughout the country, are structured so that they enforce all TSA guidelines for badging and meet Airport Security Policy as determined by each airport. And, these same systems can automatically ping FBI and other criminal databases to ascertain, in real-time, if an airport worker has been arrested, eliminating the need for 100 percent background checks of all employees on a recurrent basis.

These same systems can conduct audits recommended by the ASAC to ensure that an Authorized Signatory is in compliance with badging requirements for employees. And, in the future, as TSA explores the use of social media to track and assess emerging threats that may pose a risk to aviation, identity management systems could prove to be a valuable tool in automating this vital undertaking.

It's important to remember that the credential is just one piece of the security solution. The infrastructure must be in place, including an identity management system, to authenticate and authorize badge holders in an always-connected environment.

I want to thank the Committee again for including the security industry in this important discussion. We welcome the opportunity to contribute to improving aviation and airport security nationwide.

I look forward to your questions.

Mr. MICA. Well, thank you. We now have 9 minutes left in this vote. I have to depart. And we will not be convened before 2 o'clock, and probably sometime between 2 and 2:10 we will reconvene. So you are free to disappear until then. But we will proceed with questions at that time.

The subcommittee stands in recess.

[Recess.]

Mr. MICA. We will call the subcommittee back to order, and thank you for your patience while we conducted our votes. We have heard from all four witnesses, and now we'll proceed with some questions.

Well, let's see, Ms. Gilligan, you have been here before. As you cited today, you said you made apologies for not having some of this done and trying to get things done. April 14, 2011, you testified before us, Congress, the Transportation Committee. I know FAA has not acted on these directions as quickly or as comprehensively as this committee intended. So was yesterday Groundhog Day?

Ms. DUCKWORTH. Yes.

Mr. MICA. We keep hearing the same thing over and over. Did you want to respond?

Ms. GILLIGAN. Well, Mr. Mica, as I noted in my testimony this morning, we do understand that you are very frustrated with this. Having said that, as I also testified, there are tremendous challenges in moving this forward, not the least of which is the amount of costs that it's likely to drive. And that's why we are going to try to work with TSA, and quite honestly now, with Ms. Carroll's organization.

Mr. MICA. With Ms. Carroll's organization? Ms. Carroll, don't you have examples where this can be done fairly cost-effectively? Most of these pilots' licenses only cost—the cost is minimal. I know Disney can't be paying a fortune for their card.

Ms. CARROLL. Well, it depends. I mean—

Mr. MICA. How much would a card be?

Ms. CARROLL. A card?

Mr. MICA. A range. A range.

Ms. CARROLL. Okay. Depending on what kind of electronics are in there, what kind of security features, \$2.50.

Mr. MICA. Well, again, I want to know who has the card and who is getting access. We don't know that now.

Ms. CARROLL. Who get—that gives—

Mr. MICA. Who is in possession of the card and who is gaining the access? Are we identifying who the person is? And do we have that information embedded in the card?

Ms. CARROLL. For certain programs, yes, sir, we do.

Mr. MICA. They already have that. You already produce some of that, don't you?

Ms. CARROLL. We do. We make the U.S. green card, sir.

Mr. MICA. Does that have a fingerprint?

Ms. CARROLL. It does not have the fingerprint.

Mr. MICA. It doesn't? Well, it sure as hell should. That's another waste of money.

We sat with these people after 9/11, State Department and others. They are all producing garbage IDs. I mean, I am going to put

Ms. Duckworth on staff. She has a 1904 pilot's license, 1904 pilot's license she pulled up. It has a picture, it has the name, it has the signature. It has a physical description. Now here it's not embedded. And then it has the fingerprints. 1904.

Here is Amelia Earhart's picture, all identifying information. I'm pretty sure the other side is fingerprints. And here we are in 2016, 15 years after 9/11, we don't know who's going in and who's coming out. There is no way to ensure it.

The TWIC card, we should do another hearing on that, Transportation Worker Identification. They spent half a billion, \$500 million total? It's just incredible. Now they have to come with a driver's license. They have a card, but it doesn't have a reader. We still don't have a reader, do we, at the ports, to read them? Does anyone know? DHS know?

Mr. LAJOYE. Not as of yet.

Mr. MICA. Not as of yet. See? Fifteen years. And Mickey Mouse, or at least I called the FAA card Mickey Mouse, but the Minnie Mouse one, we know who it is.

You spoke a little bit about identity management systems, okay, but they're in very few airports or many airports? What's the status?

Ms. CARROLL. There are 21 airports. Boston Logan——

Mr. MICA. Out of 450.

Ms. CARROLL. Yeah, 21 out of 450, right.

Mr. MICA. Are they all the largest category, in the largest category?

Ms. CARROLL. DFW, Sea-Tac.

Mr. MICA. Pretty much——

Ms. CARROLL. Yeah, pretty much the bigger ones, yes, sir.

Mr. MICA. But they're not everywhere?

Ms. CARROLL. No, sir.

Mr. MICA. That's troubling, even when you have the systems. And that's interesting that the systems also can identify erratic——

Ms. CARROLL. Yes, sir. It can detect anomalies in patterns of access and where people go, and it automatically alerts security if there is an anomaly. So, for example——

Mr. MICA. But there's no requirement, and they have voluntarily put them in place.

Ms. CARROLL. Yes, sir.

Mr. MICA. But, again, we have seen that these folks target our soft areas. So you have 21, so we have another 430 locations that you can—you don't have that in place.

Iris. Where are we on iris, Ms. Gilligan?

Ms. GILLIGAN. Well, sir, I think as you know, the National Institute for Standards and Technology did issue a standard for the collection of iris.

Mr. MICA. Right. But you said there was no GSA——

Ms. GILLIGAN. Right, at this point. One of the requirements in the statute was that the system be linked to PIV requirements, and GSA has apparently——

Mr. MICA. Information, what is PIV requirements?

Ms. GILLIGAN. Ms. Carroll used it earlier, sir. I don't know what it stands for.

Ms. CARROLL. So I'm not a real technology expert, I'm more of a policy person, but the PIV card is the credential that follows the standard developed by NIST. It's a FIPS 201 standard. And so it was developed for all Federal employees so that they had—

Mr. MICA. Right. So that's the standard.

Ms. CARROLL. That's the standard, right.

Mr. MICA. But we have—we don't have that in place.

Ms. GILLIGAN. There are no systems—to your earlier point—there are not yet any approved vendors of systems to be able to read and take advantage of the iris biometric.

Mr. MICA. But you developed—I didn't mean to interrupt, but I do. Actually, I'm from New York originally. This is interesting, guys, listen. I read these old books—I collect old books—usually before 1800, printed in America. And they are little capsules of time and space. Somebody wrote them on what they observed at that time and space. This doesn't count against my time. Turn it off.

So I am reading this book, and this is back in the 1790s, and it's a guy that came from England, and he wrote his memoirs. He says: I am in New York now visiting. He said people in New York have a habit of interrupting people when they're talking. And that's over 200 years ago. I do the same thing. It's just—I think it's in the DNA or maybe the water system.

I'll give you one more quick one, and this is an aside since it's a small group. I got another book, a guy visited here 1828. Listen to this. He came to the House of Representatives. He's from England. He says, I have come to the Chamber of the House of Representatives, and he says, it's a strange body that meets there. He says, the Members stand up, he says, there's no one in the room, he says, and they give a speech, and the stenographer takes it down. Obviously, for the consumption of their constituents back home. This is before C-SPAN. This is 1828.

Then his other observation, in 1828, he says, I am here in the United States visiting, and he says, 1828 is an election, they elect the chief magistrate of the United States. They used to call them that. He says, and in this year everything circles around who shall be the next chief elected executive of the United States and nothing else gets done. Do things change much?

That was a terrible aside, but I thought I could share that with you all. There are some prerogatives as chairman.

But, again, not much has changed on this. I don't know what to do. It's troubling too to hear—you talked about TSA setting standards for IDs. Who talked about that? Carroll? Ms. Carroll?

Ms. CARROLL. Yes, sir, the ASAC recommended that the—

Mr. MICA. But they haven't.

Ms. CARROLL. Well, the recommendation just came out.

Mr. MICA. But they haven't.

Ms. CARROLL. Set standards, no.

Mr. MICA. How about that? Let's do a letter too, as a result of the hearing, staff, I won't dictate it now, we would like you to set standards for this credentialing. But that's not done yet. It just came out.

Ms. CARROLL. Yeah. I mean the recommendation to set the standards. But I mean, you know, the FIPS 201 standards, and

NIST has done significant work on setting standards for biometrics as well.

Mr. MICA. But it's all out there, but they have to adopt it. And then what was troubling is no full use of all the databases. And I think that's being corrected now. Is that right, LaJoye?

Mr. LAJOYE. Yes, sir, it is.

Mr. MICA. And I don't like to ask this, but you started giving us some numbers, like there is 70—well, there's 87,000 with no Social Security number in the base?

Mr. ROTH. That's correct. Of the 900,000 names that we pulled, there are about 87,000, or about 10 percent, had no Social Security number in the database.

Mr. MICA. And then 75,000, what was that figure?

Mr. ROTH. The 75,000, if I recall, was no passport number. And then a subset of that had no alien identification number.

Mr. MICA. So they could technically have people who are aliens working, without us knowing about it, at the airports?

Mr. ROTH. Yeah. The issue we had with TSA's data set was that there wasn't an ability, any assurance that the data could be used. So when you run it against the terrorist database or you run it—

Mr. MICA. And the 73 that you found, were they airport workers, TSA workers, combination of the above, or people who just got into secure areas?

Mr. ROTH. They would be airport workers that held a secure identification badge, in other words to be able to go into the secure areas of the airport next to the aircraft, checked baggage, that kind of thing.

Mr. MICA. I don't know why TSA can't contract—it's not that expensive—with someone who can do sort of a nonstop criminal check. Do you know any reason? We can talk to the administrator about that. That's a big gap too. And the self-reporting, as the IG pointed out, doesn't cut it, the last thing they want to do.

Do you think that's possible, Mr. LaJoye? I know you don't set policy, but—

Mr. LAJOYE. Well, Mr. Chairman, one of the things that we've recognized, along with the ASAC, is we are piloting the Rap Back program with the FBI that would allow us to get recurrent vetting with criminal records history checks similar to what we do with TSDB today. So that pilot is going to start in March, and we are hopeful that we can roll it out before the end of the year.

Mr. MICA. A couple of other quick ones before I yield.

The employee assessment is only done every 2 years. Is that correct? Or is that just for employment and then—

Mr. LAJOYE. Again, that's an interim measure we put in place, you know, until we have—

Mr. MICA. But you've been hiring people without that employee and putting them to work without that assessment completed. Is that not correct?

Mr. LAJOYE. Well, again, we put out, it was a few months ago, the requirement. We knew we wanted to work with the ASAC to get to the FBI Rap Back. But in the meantime, knowing it would take some amount of time, months, better part of a year to get that across the airports, we did require that they go out and conduct

criminal history records checks at the renewal point or every 2 years thereafter.

Mr. MICA. One of my sheriffs called me and said he had fired a couple of deputies for really serious offenses and misconduct. He said the next thing you know they were over in Daytona Beach as TSA screeners. He asked me what's going on and I couldn't tell him. But they, as we've checked, they hadn't been cleared, hadn't been properly vetted, but they could get a job.

How quickly, Ms. Gilligan, how quickly does FAA revoke a license after disqualifying information is received?

Ms. GILLIGAN. We issue the revocation based on a request by TSA that they have made a determination that someone holds a pilot certificate and is a risk to national security. So as soon as we receive the notification the process—the action is taken by our counsel's office.

Mr. MICA. But they could still use that ID with another form of ID and you'd never know who that person was.

Ms. GILLIGAN. No. When the pilot certificate is revoked, they are required to turn it in. And if they don't, we pursue that, so that we do—retrieve the pilot certificate when it's been revoked.

Mr. MICA. I want to give everyone a chance. Ms. Duckworth, we will go to you. I have more questions, unfortunately. Go ahead, Ms. Duckworth.

Ms. DUCKWORTH. I just want to follow up on that Ms. Gilligan. When you said the pilot certificate is revoked you retrieved it. What about when it's changed or they get a new certification?

Ms. GILLIGAN. I'm sorry, I was responding specifically to Mr. Mica's question. We have a process where TSA notifies us if they have determined, after someone has gotten a pilot certificate, that they now pose a risk to national security, and based on that notification we revoke that certificate.

Separately, any time a pilot gets a new rating or raises to a new level, they must present themselves to an inspector or to another designated—usually a flight instructor or other designated representative, have their photo ID. Our folks will then confirm that they demonstrate that they have met the requirements to become a commercial pilot, for example, or that they have passed their type rating in a 737, whatever it may be. And that information is transmitted then to the registry and the new certificate is issued.

Ms. DUCKWORTH. Right. But you don't take—you don't recover their old certificate with the old information.

Ms. GILLIGAN. I don't—apologize, ma'am, I actually don't know the answer to that. I thought they turn—I thought they give their old certificate when they get their new one.

Ms. DUCKWORTH. I have both my old one and my new one.

Ms. GILLIGAN. Okay. Then you're right.

Ms. DUCKWORTH. So something to take a look at.

So I'd like to take a look at the credentialing process and effectiveness and security lapses. My whole point today is just to make sure you guys get the resources and the support you need to do what you need to do to keep our people safe. And if there is something that we find out today where you need congressional help, legislative help, you need appropriations, you need something, let

us know. That's really what I am interested in, to make sure you get the resources to do what you need to do.

And so, Mr. Roth, there are many issues to be discussed today, but the central one is this. In 2011, that inspector general's report concluded that individuals who pose a threat may obtain airport badges and gain access to secured areas. Do you believe that individuals who pose a threat may still be able to obtain airport badges and gain access to secured areas today?

Mr. ROTH. Yes, I do, for a number of reasons. One is, as I highlight in my testimony, the TSA, as a regulator who has to regulate the 450 airports who make the determination with regard to criminal history, for example, can only do a fraction of the regulation that they probably need to do to check on how well the airports are adjudicating some of the criminal history. That would be one thing.

The second is that TSA's database is very, very filled with errors, and it is going to be difficult to do any kind of matching between TSA's database and, for example, the criminal history databases or even the terrorist watch list databases.

And third, the way the legislation works, it's really a box-checking exercise. You've either been convicted or not convicted of certain offenses. If you have not been convicted of those offenses, you are free to get—and you have you the ability to work in the United States—you have unrestricted access to the most secure areas within the airport. It's functionally the same level of security clearance that an individual with PreCheck would have. It isn't a holistic: We will look at this person and determine whether or not he is a threat to aviation security. Rather, if he is convicted of a certain level of crimes, he doesn't get it. Or if he is convicted, he doesn't get it. If he isn't convicted, then he gets it, regardless of what could be in his background.

Ms. DUCKWORTH. So what do you think are the most important outstanding recommendations that your office has made to TSA that have yet to be implemented?

Mr. ROTH. We are in the process of—we made six recommendations. Two of those have been closed, one of which was the most serious one, in our view, which was the lack of TSA having all the information in the TIDE database. So that's been worked out. There are a number of ones in which they are working towards getting a solution towards it. So we are satisfied that they are making progress in the right direction.

The difficulty, as I see it, is that TSA is working in a system where airports have certain authority and TSA has certain authority, and any time you have a split in authority like that, it's going to be very difficult to ensure that things don't fall through the cracks.

Ms. DUCKWORTH. Mr. LaJoye, do you have any comments on that? Or what do you need to help you to be able to meet all six of those recommendations?

Mr. LAJOYE. Well, I think at this point, Ranking Member, to the IG's point, it's just a matter of putting some technical fixes in place with data quality, is how I would characterize it. This is an intensely manual process, as you can imagine. And so errors in data, you know, inhibits our ability at times to effectively vet. And so to the extent to which we can, you know, incorporate some logic into

a system to cut down on data entries, we have gone out and we have changed our national inspection manual for all of our inspectors. When they go to a badging office, look at the original documents.

So there is a number of things we are putting in place. But with respect to the IG's open comments, I think at this point it's just a matter of putting the technical fixes in place.

Ms. DUCKWORTH. And do you have a plan for those technical fixes? Do you have the support you need to put those technical fixes into place? And what is that timeline? Are you saying that—you know, the IG is saying you are on your way to meeting those, but on your way could be 6 months or it could be 6 years.

Mr. LAJOYE. I think we're acting deliberately, sensitive to the fact that there is the cyber issues, you know, we have to—with respect to privacy. And so I couldn't characterize it as years. I'd characterize it more as months. And, again, getting back to our office I could get you specific timelines on some of them, but I can assure you there is a deliberate plan to close these in short order.

Ms. DUCKWORTH. I would love to see, and if it's all right with the chairman, a report back as to the timeline as to when they will be closing all six of the recommendations from the IG.

Mr. MICA. Okay. And we can ask the staff to follow up with questions. There will be questions submitted. And if we can get a response for the record.

Mr. LAJOYE. Absolutely.

Mr. MICA. Without objection, we will do that.

Ms. DUCKWORTH. Thank you, Mr. Chairman. I yield back.

Mr. MICA. Okay. Well, a couple more questions here. There is obviously a huge number of lost or stolen credentials. You found a lot of that, Mr. Roth?

Mr. ROTH. In our earlier audit we did find a number of essentially lost credentials. We are currently doing an audit of the SIDA badge process to see whether or not that has improved. Hopefully, we will have that audit out later this year.

Mr. MICA. And even if you had the pilot's license, which has no photo on it, has no biometric way to tell that that's the individual, and another form of ID, which might not have any form of biometric, we still don't know who's entering. Is that correct?

Mr. ROTH. My understanding is that the way the SIDA badge works in a large majority of the circumstances—

Mr. MICA. Right now I'm talking about the pilot's license.

Mr. ROTH. That I cannot comment on.

Mr. MICA. It's a fact, Ms. Gilligan. We don't know, we have no way of knowing because we still have this, as I've termed it, Mickey Mouse pilot's license. We have no biometric. We don't know who those people are. And then if it's a stolen or lost one—we had a hearing some years ago on credentials. I never realized how you can duplicate credentials. And college kid and students are incredible at reproducing these IDs. But we really don't know who that individual is unless there is a biometric.

Ms. GILLIGAN. But at this point the pilot certificate is not used to gain access in any situation.

Mr. MICA. I know. It can't be. They can use a driver's license. But the whole purpose was for us to know who is in control of the

aircraft, who the pilot is. We have had at least one instance, we saw the European, sometimes some things happen with people who have taken control of aircraft or gained access with false credentials.

Do we know with—the other thing is vetting people. I think you can screen them through metal detectors, but you need to be reviewing these individuals that are working behind a secure area—or in secure areas. And we don't do a very good job of that.

TSA has failed in vetting some of those folks, right, Mr. Roth?

Mr. ROTH. That's correct. To be more accurate, it's the airport.

Mr. MICA. What worries me after this hearing is you have just said we have got thousands of people working there. We don't even know—well, 10 percent of them we don't have Social Security numbers of. Then we have 75,000 that you mentioned, 14,000 no passports. They could be aliens.

One of my concerns is—I've seen some of the big airports on the East Coast, Chicago, they do employ a lot of folks from different nationalities, no offense, and they should be able to work. But there are people we don't know about as far as their background, and then we're not vetting them.

We don't know about Egypt, what took place there yet, do we, Mr. LaJoye, with that? They thought that the plane that was taken down supposedly by ISIS was an inside airport job. Do we know that?

Mr. LAJOYE. Well, I think that's probably worth a closed session discussing any particulars we have on that, but I am not prepared to comment beyond that, Mr. Chairman.

Mr. MICA. But a lot of things indicated it was an inside job.

And the other thing too is everything we have done with TSA is always a reaction; 9/11. We finally put in some standards. You know, everybody says private screening failed. It wasn't private screening that failed, it was the Federal Government that didn't put any standards in for the screeners. And part of that they got—the government got lobbied, don't put anything that would cost the airlines another penny. So it was the failure—it was the failure of the government to put in policies for what could not be brought on-board. There was no Federal prohibition to box cutters.

I remember when we looked at it after 9/11, the direction to pilots, and we actually read from the manual for dealing with hijacking, was to land the plane in Havana and contact the Swiss consul there. That was the instructions, to cooperate, basically, with the hijackers and then land the plane there. That was the government's instructions to the pilot.

So the government failed. And the government to me is failing to take steps. Everything we've done, the metal detectors, the shoe bomb, they saw a flaw in those. So what did we do? Of course I remember going to Italy, where they made most of the—we brought—we actually brought the metal detector capability down lower to the floor. But today most people take—have to take off their shoes unless you've got PreCheck or some situation. That's a result of Richard Reid and his—going after the diaper bomber explosives. Now we have the body scanners. It's always a reaction.

And here, again, I think they can easily determine what our most vulnerable points are. Liquid bombing, a vulnerable point,

now we all have to take our liquids out. So it's always after the fact.

Is there any progress you can report, speaking of liquid bombs? There is equipment that we went to purchase, and that sat around for a while, that could detect liquids that posed a risk, and that equipment was dumbed down or not used. Is there any current effort to buy that equipment or deploy that equipment, Mr. LaJoye?

Mr. LAJOYE. Well, again, there is various pieces of technology with respect to liquids. Some of it we do employ, some of it we have not yet deployed. We could perhaps give you a full briefing on the various different pieces of technology that are available.

Mr. MICA. I can tell the committee and staff. We looked at it, we had a whistleblower, equipment was sold to them, had that capability. They neither could train their people or operate it. So basically they disarm ability of the equipment to detect that. So we still—we can't bring things on to this day. But that equipment is available.

Let me look here. Renewal and lost. Okay. I heard that you can—can you renew your—I am going to say license, you keep saying certificate—but can you renew that license by either electronic request or by phone?

Ms. GILLIGAN. The pilot certificate is not renewed. It doesn't need to be renewed. But as Member Duckworth mentioned, most pilots add additional capabilities to their certificate over time. Any time you—

Mr. MICA. So it's just permanent? It's never—okay. Go ahead.

Ms. GILLIGAN. Well, any time you are getting—

Mr. MICA. So embedded in it would be only the information about additional capability of flying, say, certain aircraft or, like, civil versus commercial—

Ms. GILLIGAN. Right.

Mr. MICA. —versus cargo or whatever, or big planes, small planes.

Ms. GILLIGAN. That's right. Every time someone adds a capability to their credential—

Mr. MICA. That's interesting, because provided by Ms. Duckworth, again, incredible research—in fact, maybe we could divide some of the staff money to add it on to your pay for the work you've done on this one. But this even has license renewals here—

Ms. GILLIGAN. That would likely have been the medical. So pilots do renew their medical certificate.

Mr. MICA. Inspector's endorsement. That's what it says. And the renewal. We don't have that—there is no renewal.

Ms. GILLIGAN. We don't require renewal.

Mr. MICA. Okay. Okay. Just, again, and lost, you have any information on lost or stolen credentials, Mr. Roth?

Mr. ROTH. Again, the airports have an obligation when a SIDA badge is reported lost or stolen or that employee quits, leaves, to turn it off.

Mr. MICA. And they are required to notify TSA?

Mr. LAJOYE. They're required to notify the airport, Mr. Chairman, where then the airport is required to immediately deactivate the badge.

Mr. MICA. But do you get a notification on them?

Mr. LAJOYE. We would not if it's a lost or stolen badge. Again, that would happen to the airport. Now, we do inspect, right, because every airport they have thresholds they can't exceed. So we went back—

Mr. MICA. There is a law or regulation that says when 7 percent of the credentials are compromised they have to reissue all new. Is that—

Mr. LAJOYE. We can—I mean, I can brief you specifically on what the requirements are, but it's lower than what you just cited, Mr. Chairman. But we went back over a 5-year period, understanding this is an area where the majority of airports are really very compliant because the cost of noncompliance is steep. It's exceedingly expensive for them to rebadge their population. So we went back over 5 years, almost 450 airports, and we only had 23 instances of airports having to rebadge any part of their population.

So, again, this is really an area where the airports have a high level of compliance with respect to maintaining control of those lost and stolen badges.

Mr. MICA. So you're basically relying mostly on a driver's license for identification, right?

Mr. LAJOYE. I'm referring to SIDA badges that are lost.

Mr. MICA. Well, let's say for a passenger—or for a pilot, because the pilot has an ID that doesn't have a picture and information.

Ms. GILLIGAN. But, Mr. Chairman, the pilots do have SIDA badges.

Mr. MICA. Yes.

Ms. GILLIGAN. Pilots are vetted through the airport system, just as all employees are.

Mr. MICA. But they're all different, as we've heard.

Ms. GILLIGAN. There are differences. And as I think Ms. Carroll makes the case, there is value in looking at how to perhaps refine that process. But I don't want to leave the impression that pilots aren't—

Mr. MICA. And some of this too is—I can't blame you all totally because I have seen what happens. The airports lobby for keeping everything they're doing, and they don't want to change it, my God, you can't change it. The airlines are just as bad. Oh, no, they can't do this. You can't require that. There can't be standardization. They're just as bad. And then some of you are left in the lurch. So I'll give you that much credit.

But we still have credentials, as I called it, in chaos. And somehow it's gotten us to this stage, but it's in spite—we have been very lucky and fortunate so far. I try to stay a little bit ahead of the curve. I think we need to have a sitdown with the new Administrator again. He was good to come in at the beginning. I know he's trying to institute some changes and reforms, things that make sense. But I think there are some of these items that we need to go over.

I think we probably should look at some of the results—sometimes we do these hearings and nothing gets done. But what we might do, staff on both sides, make a list of some of these items. And then they have we have authorizers, Mr.—from New York—

Katko, he is an authorizer. He has also passed a couple of bills. We are not an authorizing committee. We are investigation and oversight. But if we just look at these and do nothing, not much comes as a positive result.

So if we could, staff, let's put together, work with the minority, the things that we have uncovered here today that we could.

And if you get a chance, we will sit down with the Administrator and see where we could do more.

FAA, we'll have another Groundhog Day in a couple of years and we'll hear that they're on their way. But they also have some constraints, I know. And then the private sector has the solutions.

Don't you have the solutions, Ms. Carroll?

Ms. CARROLL. Yes, sir, we do. And all we want to do is help in whatever way we can.

Mr. MICA. You are doing both the fingerprint and iris. You have that capability?

Ms. CARROLL. Yes, sir.

Mr. MICA. You have readers for both?

Ms. CARROLL. We have readers for all, yes, sir. And we have the systems to overlay.

Mr. MICA. I think the staff, when we were putting this together, 15 years ago I was at some of the European airports, and they had the finger and iris in operation. That's 15 years ago.

Ms. CARROLL. Well, sir, just a point of clarification. In the United States, especially, fingerprints seems to be the default because they have to do criminal background checks and things like that. And so most of our databases for criminal background checks are fingerprints. And so that seems to be—especially for workers.

Mr. MICA. For a passenger. Like I have PreCheck.

Ms. CARROLL. Perfect. Iris is a good solution for passengers because of the—

Mr. MICA. I think CLEAR might have that. Does CLEAR have that?

Ms. CARROLL. I'm not sure. I'm not sure. Yeah.

Mr. MICA. They may have. And we've looked at turning that over to the private sector, all of the people who could qualify for PreCheck or credentialing, and then let TSA keep some of the rest of the mix. But, again, we don't know who is getting on. We don't know where the credentials are. The credentials are lacking information.

Let's see if I have got any final questions. We will be submitting, as I said, some questions for you to respond to.

One last question about—we rely quite a bit on a driver's license. The Feds have set some REAL ID standards, I guess, and I guess there are still some States in noncompliance. Where are we with that, Mr. LaJoye?

Mr. LAJOYE. Some of the initial enforcement of that will begin in 2018, and final enforcement will begin in 2020, Mr. Chairman, you know, at the point—

Mr. MICA. I'm sorry? 2000—give me the—

Mr. LAJOYE. Some of the initial enforcement of the REAL ID-compliant driver's license to gain access to the checkpoint will begin in 2018, with final enforcement beginning in 2020 on that.

Mr. MICA. But we're still 2 years out. But you're accepting the flawed IDs now.

Mr. LAJOYE. Well, again, I mean, it's—

Mr. MICA. It's noncompliant. Yes. I mean, yes, you are.

Mr. LAJOYE. Well, again, we will start enforcement of that in 2 years. It gives time for States to—

Mr. MICA. We can pick out the States you should enforce it.

Ms. DUCKWORTH. Like Illinois.

Mr. MICA. Illinois.

And then final for Ms. Gilligan. When does FAA expect to establish a pilot records database?

Ms. GILLIGAN. We're working closely, actually, sir, with one of the representatives from the family groups from Colgan who has a technical background.

Mr. MICA. This is way, way back.

Ms. GILLIGAN. The requirement for the pilot records database was in the FAA Extension and Safety Act of 2010.

Mr. MICA. And what year is this?

Ms. GILLIGAN. 2016. So we are working to establish—we have done a pilot program. We do understand what is required. The dilemma is that there are a number of kinds of records that airlines have kept over the years, including paper records and microfiche and—

Mr. MICA. But you can set standards—

Ms. GILLIGAN. Yes, sir, but—

Mr. MICA. —for the records. Have you?

Ms. GILLIGAN. Set standards for the records?

Mr. MICA. For what is required as far as keeping for a database.

Ms. GILLIGAN. Yes, we have informed the airlines—

Mr. MICA. And then it can be electronically transmitted.

Ms. GILLIGAN. We have informed the airlines of the records that they need to maintain in accordance with the statute, and that began in 2011 after the passage of the statute.

Mr. MICA. But yet we still don't have a database.

Ms. GILLIGAN. We have not been able to establish the integrated database at this point.

Mr. MICA. Again, it's just very, very, very, very, very, very frustrating.

Anything else, Ms. Duckworth?

Ms. DUCKWORTH. Not at this time, Mr. Chairman.

Mr. MICA. Okay. I will ask the staff to go through and see what questions we want to submit. We appreciate your response for the record. We leave leave the record open for—instead of 5 days, let's change it to 10 days, because we'll submit a bunch of questions to them that have not been answered here.

Mr. MICA. We appreciate your participation. Our intent is to try to do better. And we have a responsibility for oversight and making certain we move this process forward and keep us safe and secure.

There being no further business before the subcommittee, this subcommittee hearing is adjourned.

[Whereupon, at 2:51 p.m., the subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Question#:	1
Topic:	TSA Warehouses
Hearing:	Securing Our Skies: Oversight of Aviation Credentials
Primary:	The Honorable John L. Mica
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: Please provide the Committee a list and current inventory of all TSA warehouses as of March 1, 2016.

Response:

Warehouses as of March 1 2016	Number of Assets	Value
Township, NJ	877	\$3,770,919.89
Springfield, VA	3,685	\$16,819,661.34
Coppell, TX	1,222	\$114,616,940.84
Total	5,784	\$135,207,522.07

Question: Please provide the Committee with all TSA Quarterly Warehouse Inventory Reports issued from January 2012 through the present.

Response: Attached are inventory summaries by quarter from FY 2012 to March 1, 2016 (which is a partial quarter) of the value of items in the three Transportation Security Administration (TSA) warehouses.

Since the findings of OIG-10-14, "*Management of the Transportation Security Administration's Logistics Center*" in 2009, the TSA has made substantial progress in the processes, internal controls, and standard operating procedures related to the operations of the agency's warehouses. This effort has reduced the need for warehouse space substantially.

Previously, TSA had three separate warehouses in the Dallas, TX area which were acquired to accommodate the initial quick growth of the agency and to house equipment designated for disposal. In response to the findings, TSA created a disposal plan and in 2012 started its space reduction goals by closing the Transportation Logistics Center (TLC) 2 warehouse (150,000 square feet). In 2014, TSA met another one of its space reduction goals by simultaneously closing the TLC 1 (233,740 square feet) and the TLC 3 (109,750 square) and consolidating all of the equipment that was stored in the previous three warehouses into a single leased warehouse, the Transportation Security Administration Logistics Center (TSALC), in Coppell Texas.

Question#:	1
Topic:	TSA Warehouses
Hearing:	Securing Our Skies: Oversight of Aviation Credentials
Primary:	The Honorable John L. Mica
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

This consolidation effort resulted in TSA achieving an 183,490 square feet reduction in warehouse space. Also, by leasing the TSALC, TSA was able to close down the TSA Oklahoma warehouse space moving TSA's Office of Training Division Federal Flight Deck Officer Program and their Specialized Security Training (SST), Threat Mitigation Engineering and Image program to the TSALC. This resulted in an additional warehouse space reduction of 48,000 square feet.

Additionally, to further reduce inventory levels, TSA has refined requirements for holding safety stock (i.e., support for unplanned warehouse expansions, recurring and non-recurring special events, and unplanned replacement requirements) and was able to further reduce the warehouse inventory for this purpose from an average of 700 units on hand to approximately 250 units. To ensure inventory levels remain commensurate with TSA operational requirements, TSA performs annual reviews of operational requirements, including planned technology purchases and disposals, and makes inventory adjustments based on that assessment. The results of these reviews can be briefed to the Committee, if desired.

Question#:	2
Topic:	TSA Salaries
Hearing:	Securing Our Skies: Oversight of Aviation Credentials
Primary:	The Honorable John L. Mica
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: What are the average and median yearly salaries for a TSA employee that works within a 15 mile radius of DC?

Response: The average and median yearly salaries for a Transportation Security Administration employee that works within a 15 mile radius of DC is shown in the following table:

	Mean	Median
15 Mile Radius of DC	\$ 95,743	\$ 95,883

Question: What are the average and median salaries of a TSO?

Response: The average and median yearly salaries for the Transportation Security Administration's Transportation Security Officers are shown in the following table:

Category	Mean	Median
Transportation Security Officer (TSO)	\$38,732	\$38,753
Lead Transportation Security Officer (LTSO)	\$46,673	\$45,237
Supervisory Transportation Security Officer (STSO)	\$54,434	\$53,304
Behavior Detection Officer (BDO)	\$47,389	\$45,936
Supervisory Behavior Detection Officer (SBDO)	\$56,567	\$54,712

Question#:	3
Topic:	TSA's FLETC Training
Hearing:	Securing Our Skies: Oversight of Aviation Credentials
Primary:	The Honorable John L. Mica
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: To what extent will TSA's FLETC training utilize simulation over live-fire ammunition?

Response: The Transportation Security Administration's (TSA) Federal Air Marshal Training Program-I does not currently use any simulation-based training in place of live-fire ammunition evolutions. The training program does employ marking cartridge (Ammunition), or airsoft for force-on-force training. There is also a block of instruction that utilizes laser-based training weapons for judgment pistol shooting.

The Federal Flight Deck Officer (FFDO) training program also does not use any simulation-based training to replace live-fire exercises. TSA conducts training on use of force using laser-based weapons platforms in a simulated flight deck.

Question: How many new hires at TSA are trained to operate a handgun?

Response: The Transportation Security Administration's (TSA) Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) has not conducted hiring of Federal Air Marshals since 2011, and has not on-boarded any new hires to date in FY16. Therefore, no new hire employees were trained by TSA to operate a handgun during FY15.

The OLE/FAMS also has five Supervisory Transportation Security Specialists (Law Enforcement) assigned to the Physical Security Section, with oversight responsibility of the contracted TSA Guard Force. These Supervisory TSS-LEs transferred from other Federal law enforcement positions and were certified to carry and use firearms prior to entering service with TSA. They are required to qualify and exhibit proficiency with their service weapons on a quarterly basis.

The TSA Office of Inspection (OOI) employs a cadre of criminal investigators (OPM series 1811) who are authorized to carry firearms. In calendar years 2014 and 2015, the TSA OOI hired four and eight criminal investigators, respectively. All of these new hires transferred from other Federal law enforcement positions and were certified to carry and use firearms prior to entering service with TSA. Criminal Investigators working in OOI are required to qualify and exhibit proficiency with their service weapons on a quarterly basis.

Question: How many rounds of ammunition did TSA use in FY 2015?

Response: The Transportation Security Administration used a total of 9,076,323 rounds of ammunition in Fiscal Year 2015.

Question#:	4
Topic:	Searches and Badge Checks of Airport Workers
Hearing:	Securing Our Skies: Oversight of Aviation Credentials
Primary:	The Honorable John L. Mica
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: What has TSA found in regards to the recently implemented random searches and badge checks of airport workers?

Response: Airport and airline employee screening is an important part of the Transportation Security Administration's (TSA) security mission and mitigates the insider threat. Since the TSA has implemented increased employee screening efforts, the number of employees screened has grown from 3.3 million in 2014 to 16.9 million in 2015. Through the employee screening program, TSA officers continue to find airport and airline employees attempting to access secure areas of the airport with dangerous items in their possession, such as firearms, knives, pepper spray, and other threat items. TSA officers during the course of their screening activities also encounter employees using their access badges to bypass checkpoint screening when traveling as passengers and violating various other access control policies.

Question: What have been the early findings of these efforts?

Response: TSA has increased employee screening/inspection efforts, reduced in the total number of airport access points, enhanced Insider Threat training, and initiated a pilot at various locations which automates and provides real time Criminal History Recurrent Checks (CHRC). These combined efforts have increased the ability to deter, detect, and disrupt a potential terror attack by an insider threat. The Transportation Security Administration (TSA) asserts that although there may be instances when an employee attempts to circumvent the screening process, TSA is confident that the increased number of random employee searches has strengthened the perception of the airport employee populations that they may receive screening when accessing the airport for work. For example, in calendar year 2015, a screening operation designed to mitigate the insider threat, called "Playbook: Insider Threat", generated 547 total incidents involving aviation workers (AWs).

When comparing AW incidents against the total number of AWs screened by month, the incident occurrence rate decreased by 77 percent, from .01373 percent in January 2015 to .00249 percent in December 2015.

Question: Do any airports conduct 100% screening of workers for prohibited items? If so, which airports?

Response: Orlando International Airport (MCO) and Miami International Airport (MIA) are the only federalized airports that conduct 100 percent screening of workers for

Question#:	4
Topic:	Searches and Badge Checks of Airport Workers
Hearing:	Securing Our Skies: Oversight of Aviation Credentials
Primary:	The Honorable John L. Mica
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

dangerous or illegal items. Atlanta International Airport (ATL) conducts a very high level of employee screening.

Question#:	5
Topic:	Whistleblower Protections
Hearing:	Securing Our Skies: Oversight of Aviation Credentials
Primary:	The Honorable John L. Mica
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: What policies are currently in place to inform employees of their rights as whistleblowers?

Response: Question 5 seeks information beyond the scope of topics that I, in my capacity as Deputy Assistant Administrator for the Office of Security Operations, have personal knowledge of, and/or are beyond the scope of the February 3, 2016 hearing entitled “Securing Our Skies: Oversight of Aviation Credentials.” Nevertheless, TSA seeks to accommodate the requests of this Committee. If the Committee should choose to include this question in a letter to TSA, we will be happy to respond appropriately.

Question: How often does TSA require employees to complete training on whistleblower protections?

Response: Question 5 seeks information beyond the scope of topics that I, in my capacity as Deputy Assistant Administrator for the Office of Security Operations, have personal knowledge of, and/or are beyond the scope of the February 3, 2016 hearing entitled “Securing Our Skies: Oversight of Aviation Credentials.” Nevertheless, TSA seeks to accommodate the requests of this Committee. If the Committee should choose to include this question in a letter to TSA, we will be happy to respond appropriately.

Question: What is the punishment at TSA for retaliating against a whistleblower?

Response: Question 5 seeks information beyond the scope of topics that I, in my capacity as Deputy Assistant Administrator for the Office of Security Operations, have personal knowledge of, and/or are beyond the scope of the February 3, 2016 hearing entitled “Securing Our Skies: Oversight of Aviation Credentials.” Nevertheless, TSA seeks to accommodate the requests of this Committee. If the Committee should choose to include this question in a letter to TSA, we will be happy to respond appropriately.

Question: Is TSA in compliance with the Whistleblower Protection Enhancement Act's standards for non-disclosure agreements?

Response: Question 5 seeks information beyond the scope of topics that I, in my capacity as Deputy Assistant Administrator for the Office of Security Operations, have personal knowledge of, and/or are beyond the scope of the February 3, 2016 hearing entitled “Securing Our Skies: Oversight of Aviation Credentials.” Nevertheless, TSA seeks to accommodate the requests of this Committee. If the Committee should choose to include this question in a letter to TSA, we will be happy to respond appropriately.

Question#:	6
Topic:	Administrative Leave 2
Hearing:	Securing Our Skies: Oversight of Aviation Credentials
Primary:	The Honorable John L. Mica
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: In the past year, how many TSA employees have been placed on administrative leave as a result of an ongoing investigation?

Response: Question 6 seeks information beyond the scope of topics that I, in my capacity as Deputy Assistant Administrator for the Office of Security Operations, have personal knowledge of, and/or are beyond the scope of the February 3, 2016 hearing entitled “Securing Our Skies: Oversight of Aviation Credentials.” Nevertheless, TSA seeks to accommodate the requests of this Committee. If the Committee should choose to include this question in a letter to TSA, we will be happy to respond appropriately.

Question: How long was/is each individual on administrative leave?

Response: Question 6 seeks information beyond the scope of topics that I, in my capacity as Deputy Assistant Administrator for the Office of Security Operations, have personal knowledge of, and/or are beyond the scope of the February 3, 2016 hearing entitled “Securing Our Skies: Oversight of Aviation Credentials.” Nevertheless, TSA seeks to accommodate the requests of this Committee. If the Committee should choose to include this question in a letter to TSA, we will be happy to respond appropriately.

Question: In the past year, how many security clearances have been revoked from TSA employees?

Response: Question 6 seeks information beyond the scope of topics that I, in my capacity as Deputy Assistant Administrator for the Office of Security Operations, have personal knowledge of, and/or are beyond the scope of the February 3, 2016 hearing entitled “Securing Our Skies: Oversight of Aviation Credentials.” Nevertheless, TSA seeks to accommodate the requests of this Committee. If the Committee should choose to include this question in a letter to TSA, we will be happy to respond appropriately.

Question#:	7
Topic:	Administrative Leave 2
Hearing:	Securing Our Skies: Oversight of Aviation Credentials
Primary:	The Honorable John L. Mica
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: How many employees at TSA are currently on administrative leave as a result of an ongoing investigation?

Response: Question 7 seeks information beyond the scope of topics that I, in my capacity as Deputy Assistant Administrator for the Office of Security Operations, have personal knowledge of, and/or are beyond the scope of the February 3, 2016 hearing entitled “Securing Our Skies: Oversight of Aviation Credentials.” Nevertheless, TSA seeks to accommodate the requests of this Committee. If the Committee should choose to include this question in a letter to TSA, we will be happy to respond appropriately.

Question#:	8
Topic:	TSA Operating System
Hearing:	Securing Our Skies: Oversight of Aviation Credentials
Primary:	The Honorable John L. Mica
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: What operating system does TSA use?

How much does TSA spend annually on maintaining IT systems?

Have you had a penetration test done on your network in the last year?

(If YES) Follow-up: Do you know how long the white hat hackers were in the Agency's network before they were discovered?

Response: Question 8 seeks information beyond the scope of topics that I, in my capacity as Deputy Assistant Administrator for the Office of Security Operations, have personal knowledge of, and/or are beyond the scope of the February 3, 2016 hearing entitled "Securing Our Skies: Oversight of Aviation Credentials." Nevertheless, TSA seeks to accommodate the requests of this Committee. If the Committee should choose to include this question in a letter to TSA, we will be happy to respond appropriately.

Question#:	9
Topic:	Presumption of Openness
Hearing:	Securing Our Skies: Oversight of Aviation Credentials
Primary:	The Honorable John L. Mica
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: The President issued a memorandum in 2009 directing agencies to adopt a presumption of openness. Has TSA adopted a presumption of openness?

If so, how has that changed FOIA operations at your agency?

Can you provide some examples of records that have been released since your agency adopted this presumption of openness that you would not have otherwise released?

How does TSA apply the presumption of openness to the deliberative process privilege when responding to FOIA requests? How does TSA determine that records need to be withheld under deliberative process privilege?

Response: Question 9 seeks information beyond the scope of topics that I, in my capacity as Deputy Assistant Administrator for the Office of Security Operations, have personal knowledge of, and/or are beyond the scope of the February 3, 2016 hearing entitled "Securing Our Skies: Oversight of Aviation Credentials." Nevertheless, TSA seeks to accommodate the requests of this Committee. If the Committee should choose to include this question in a letter to TSA, we will be happy to respond appropriately.

Question#:	10
Topic:	FOIA Training
Hearing:	Securing Our Skies: Oversight of Aviation Credentials
Primary:	The Honorable John L. Mica
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: How much training did your FOIA staff receive in the past year?

Response: Question 10 seeks information beyond the scope of topics that I, in my capacity as Deputy Assistant Administrator for the Office of Security Operations, have personal knowledge of, and/or are beyond the scope of the February 3, 2016 hearing entitled “Securing Our Skies: Oversight of Aviation Credentials.” Nevertheless, TSA seeks to accommodate the requests of this Committee. If the Committee should choose to include this question in a letter to TSA, we will be happy to respond appropriately.

Question: How much training does agency-wide staff receive on FOIA?

Response: Question 10 seeks information beyond the scope of topics that I, in my capacity as Deputy Assistant Administrator for the Office of Security Operations, have personal knowledge of, and/or are beyond the scope of the February 3, 2016 hearing entitled “Securing Our Skies: Oversight of Aviation Credentials.” Nevertheless, TSA seeks to accommodate the requests of this Committee. If the Committee should choose to include this question in a letter to TSA, we will be happy to respond appropriately.

Question: How much training does agency-wide staff receive on federal record responsibilities?

Response: Question 10 seeks information beyond the scope of topics that I, in my capacity as Deputy Assistant Administrator for the Office of Security Operations, have personal knowledge of, and/or are beyond the scope of the February 3, 2016 hearing entitled “Securing Our Skies: Oversight of Aviation Credentials.” Nevertheless, TSA seeks to accommodate the requests of this Committee. If the Committee should choose to include this question in a letter to TSA, we will be happy to respond appropriately.

Question#:	11
Topic:	Federal Records Act Violations
Hearing:	Securing Our Skies: Oversight of Aviation Credentials
Primary:	The Honorable John L. Mica
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: In the last 5 years, have there been any violations or allegations of violations of the Federal Records Act? If so, what were they?

Response: Question 11 seeks information beyond the scope of topics that I, in my capacity as Deputy Assistant Administrator for the Office of Security Operations, have personal knowledge of, and/or are beyond the scope of the February 3, 2016 hearing entitled “Securing Our Skies: Oversight of Aviation Credentials.” Nevertheless, TSA seeks to accommodate the requests of this Committee. If the Committee should choose to include this question in a letter to TSA, we will be happy to respond appropriately.

FY12 Q1		
Warehouse	Number of Assets	Value
Atlantic City, NJ	1,950	\$2,697,966.80
Springfield, VA	5,567	\$27,164,873.91
Dallas, TX	5,141	\$238,490,232.33
Totals	12,658	\$268,353,073.04

FY12 Q2		
Warehouse	Number of Assets	Value
Atlantic City, NJ	1,760	\$4,308,049.48
Springfield, VA	6,195	\$27,378,912.14
Dallas, TX	3,800	\$159,248,032.97
Totals	11,755	\$190,934,994.59

FY12 Q3		
Warehouse	Number of Assets	Value
Atlantic City, NJ	1,553	\$4,097,733.73
Springfield, VA	4,394	\$20,727,851.57
Dallas, TX	3,191	\$149,796,530.56
Totals	9,138	\$174,622,115.86

FY12 Q4		
Warehouse	Number of Assets	Value
Atlantic City, NJ	1,065	\$3,559,133.69
Springfield, VA	7,246	\$22,326,069.26
Dallas, TX	2,803	\$145,977,961.74
Totals	11,114	\$171,863,164.69