

# HOW TSA CAN IMPROVE AVIATION WORKER VETTING

---

---

## HEARING BEFORE THE SUBCOMMITTEE ON TRANSPORTATION SECURITY OF THE COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

JUNE 16, 2015

**Serial No. 114-21**

Printed for the use of the Committee on Homeland Security



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

U.S. GOVERNMENT PUBLISHING OFFICE

96-167 PDF

WASHINGTON : 2015

---

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

## COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas	BENNIE G. THOMPSON, Mississippi
PETER T. KING, New York	LORETTA SANCHEZ, California
MIKE ROGERS, Alabama	SHEILA JACKSON LEE, Texas
CANDICE S. MILLER, Michigan, <i>Vice Chair</i>	JAMES R. LANGEVIN, Rhode Island
JEFF DUNCAN, South Carolina	BRIAN HIGGINS, New York
TOM MARINO, Pennsylvania	CEDRIC L. RICHMOND, Louisiana
LOU BARLETTA, Pennsylvania	WILLIAM R. KEATING, Massachusetts
SCOTT PERRY, Pennsylvania	DONALD M. PAYNE, JR., New Jersey
CURT CLAWSON, Florida	FILEMON VELA, Texas
JOHN KATKO, New York	BONNIE WATSON COLEMAN, New Jersey
WILL HURD, Texas	KATHLEEN M. RICE, New York
EARL L. "BUDDY" CARTER, Georgia	NORMA J. TORRES, California
MARK WALKER, North Carolina	
BARRY LOUDERMILK, Georgia	
MARTHA MCSALLY, Arizona	
JOHN RATCLIFFE, Texas	
DANIEL M. DONOVAN, JR., New York	

BRENDAN P. SHIELDS, *Staff Director*  
JOAN V. O'HARA, *General Counsel*  
MICHAEL S. TWINCHEK, *Chief Clerk*  
I. LANIER AVANT, *Minority Staff Director*

---

## SUBCOMMITTEE ON TRANSPORTATION SECURITY

JOHN KATKO, New York, *Chairman*

MIKE ROGERS, Alabama	KATHLEEN M. RICE, New York
EARL L. "BUDDY" CARTER, Georgia	WILLIAM R. KEATING, Massachusetts
MARK WALKER, North Carolina	DONALD M. PAYNE, JR., New Jersey
JOHN RATCLIFFE, Texas	BENNIE G. THOMPSON, Mississippi ( <i>ex officio</i> )
MICHAEL T. MCCAUL, Texas ( <i>ex officio</i> )	

KRISTA P. HARVEY, *Subcommittee Staff Director*  
DENNIS TERRY, *Subcommittee Clerk*  
VACANCY, *Minority Subcommittee Staff Director*

# CONTENTS

	Page
STATEMENTS	
The Honorable John Katko, a Representative in Congress From the State of New York, and Chairman, Subcommittee on Transportation Security:	
Oral Statement .....	1
Prepared Statement .....	3
The Honorable Kathleen M. Rice, a Representative in Congress From the State of New York, and Ranking Member, Subcommittee on Transportation Security .....	3
WITNESSES	
Mr. John Roth, Inspector General, U.S. Department of Homeland Security:	
Oral Statement .....	5
Prepared Statement .....	7
Ms. Stacey Fitzmaurice, Deputy Assistant Administrator, Office of Intelligence and Analysis, Transportation Security Administration, U.S. Department of Homeland Security .....	10
Ms. Jennifer A. Grover, Director, Transportation Security and Coast Guard Issues, Homeland Security and Justice Team, U.S. Government Accountability Office:	
Oral Statement .....	12
Prepared Statement .....	13



## HOW TSA CAN IMPROVE AVIATION WORKER VETTING

---

Tuesday, June 16, 2015

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

The subcommittee met, pursuant to call, at 10:06 a.m., in Room 311, Cannon House Office Building, Hon. John Katko [Chairman of the subcommittee] presiding.

Present: Representatives Katko, Rogers, Carter, Ratcliffe, McCaul, Rice, Keating, and Payne.

Mr. KATKO. The Homeland Security Subcommittee on Transportation Security will come to order.

The subcommittee is meeting today to hear testimony on improving aviation worker vetting by TSA. I now recognize myself for an opening statement.

I would like to welcome everyone to today's hearing on how TSA can improve aviation worker vetting. Since the start of the Congress, my subcommittee has actively engaged and examined a number of alarming aspects relating to TSA's operations, policies, and procedures. Through hearings, oversight inquiries, and legislation, we have been working to get to the bottom of these issues and raise awareness of the urgent need to fix them. Recent revelations that the TSA cleared for employment individuals with potential ties to terrorism demonstrate the dire need for improved, streamlined procedures at TSA. The findings released by the Department of Homeland Security inspector general over the last few weeks are, indeed, alarming.

In May, the inspector general released a report that found that TSA did not have the appropriate controls in place to ensure that screening equipment has necessary maintenance work performed. A few weeks ago, news outlets reported test results showing that screeners failed to detect prohibited threat items 96 percent of the time. Just last week, we learned that 73 airport employees with potential ties to terrorism were issued credentials which allowed them to get access to secure areas of airports. These more recent findings come out on the heels of revelations earlier this year of security breaches by employees at major U.S. airports involving a Nation-wide gun-smuggling ring and an employee of the FAA bypassing security and flying with a loaded firearm using his SIDA badge.

More recently, we learned of a drug trafficking ring operating out of the airport in Oakland, California. All of these findings individ-

ually are concerning. In the aggregate, well, they just shake the public's confidence and only further demonstrate the need for steady leadership at TSA to work through the many issues that plague this agency.

This committee will continue to lead efforts to close security loopholes and ensure the continuing safety and security of our Nation's aviation system. The purpose of today's hearing is to thoroughly examine the identified security gaps highlighted in the most recent IG report about aviation worker vetting and find ways to improve the vetting process to ensure that these vulnerabilities are addressed and the American people can feel safe and secure when traveling.

Aviation workers are supposed to be thoroughly vetted due to their continuing access to sensitive areas of airports and the fact that they hold a position of trust within the transportation system. However, as the IG report has found so clearly, there are significant shortfalls in the vetting policies for aviation workers. For example, the IG found that TSA does not have access to all the data it may need to thoroughly check an aviation worker's potential ties to terrorism. However, what is even more alarming is that a memo was sent to the TSA administrator last year noting the need for additional information. TSA has still yet to resolve this gap a year later. The report also found that airports do not match the expiration date of an employee's credentials to the expiration of their legal work authorization in the United States.

Again, while TSA stated they are working to resolve these issues by the end of the calendar year, it raises serious concerns that this gap exists in the first place. Therefore, I have sponsored H.R. 2750, the Improved Security Vetting for Aviation Workers Act of 2015, which I introduced last week along with Chairman McCaul and Ranking Member Rice and Congressman Payne, to close these security gaps and ensure the safety and security of the transportation networks. The reality is in this post-9/11 world that the terrorist threat is metastasizing. We, as a Nation, must remain responsive to any holes in the security of our transportation systems and ensure that the protocols keep pace with the ever-evolving threat landscape.

Improving the vetting of the aviation workers who have access to these sensitive areas of airports can help close another back-door vulnerability at our Nation's airports. At today's hearing, we have representatives from the TSA, the DHS inspector general himself, and GAO to address how the recommendations highlighted in the report can be implemented, and what tools are needed to improve the security at our Nation's airports. I look forward to hearing their testimony and having a meaningful dialogue on how we can better protect this vital transportation mode and keep aviation safe and secure for the American people.

The Chair now recognizes the Ranking Minority Member of the subcommittee, the gentlelady from New York, Miss Rice, for any statement she may have.

[The statement of Chairman Katko follows:]

## STATEMENT OF CHAIRMAN JOHN KATKO

I would like to welcome everyone to today's hearing on how TSA can improve aviation worker vetting. Since the start of this Congress, my subcommittee has actively examined a number of alarming aspects related to TSA's operations, policies, and procedures. Through hearings, oversight inquiries, and legislation, I have been working to get to the bottom of these issues and raise awareness of the urgent need to fix them. Recent revelations that the TSA cleared for employment individuals with potential ties to terrorism demonstrate the dire need for improved, streamlined procedures at the TSA.

The findings released by the Department of Homeland Security Inspector General over the last few weeks are alarming. In May, the Inspector General released a report that found that TSA did not have the appropriate controls in place to ensure that screening equipment has necessary maintenance work performed. A few weeks ago news outlets reported test results showing that screeners failed to detect prohibited threat items 96% of the time, and just last week we learned that 73 airport employees with potential ties to terrorism were issued credentials granting them access to work in the secure areas of our Nation's airports. These more recent findings come on the heels of revelations earlier this year of security breaches by employees at major U.S. airports involving a Nation-wide gun-smuggling ring and an employee of the FAA bypassing security and flying with a loaded firearm using his SIDA badge. All of these findings individually are concerning, and, in the aggregate, shake public confidence and only further demonstrate the need for steady leadership at TSA to work through the many issues that plague the agency.

This committee will continue to lead efforts to close security loopholes and ensure the continuing safety and security of our Nation's aviation system. The purpose of today's hearing is to thoroughly examine the identified security gaps highlighted in the most recent IG report about aviation worker vetting and find ways to improve the vetting process to ensure that these vulnerabilities are addressed and the American people can feel safe and secure when traveling.

Aviation workers are supposed to be thoroughly vetted, due to their continuing access to sensitive areas of airports and the fact they hold a position of trust within the transportation system. However, the IG report found significant shortfalls in the vetting policies for aviation workers. For example, the IG found that TSA does not have access to all of the data it may need to thoroughly check an aviation worker's potential ties to terrorism. However, what is even more alarming is that a memo was sent to the TSA administrator last year noting the need for additional information, and TSA has still yet to resolve this gap. The report also found that airports do not match the expiration date of an employee's credential to the expiration of their legal work authorization in the United States. Again, while TSA stated they are working to resolve this issue by the end of the calendar year, it raises serious concerns that this gap exists in the first place.

That is why I have sponsored H.R. 2750, the Improved Security Vetting for Aviation Workers Act of 2015, which I introduced last week, along with Chairman McCaul, Ranking Member Rice, and Congressman Payne to close these security gaps, and ensure the safety and security of the transportation networks.

The reality is that in this post-9/11 world, the terrorist threat is metastasizing and we, as a Nation, must remain responsive to any holes in the security of our transportation systems and ensure that the protocols keep pace with the ever-evolving threat landscape. Improving the vetting of the aviation workers who have access to these sensitive areas of airports can help close another backdoor vulnerability at our Nation's airports.

At today's hearing, we have representatives from TSA, the DHS inspector general, and GAO to address how the recommendations highlighted in the report can be implemented and what tools are needed to improve the security at our Nation's airports. I look forward to hearing their testimony and having a meaningful dialogue on how we can better protect this vital transportation mode and keep aviation safe and secure for the American people.

Miss RICE. Thank you, Mr. Chairman. Thank you for convening this hearing. We have an important question to answer today: How can we do a better job vetting aviation workers? How can we do a better job ensuring that criminals and terrorists cannot get a job in one of our airports and gain access to secure areas? Clearly, if a terrorist were to penetrate an airport in that way, the results could be catastrophic.

We have to assume that right now someone is trying to do just that. We have to assume that we can prevent it. We have to keep working together aggressively and proactively to strengthen our security, find and close the gaps, and stay one step ahead.

TSA is responsible for vetting diverse groups of people, from the Transit Worker Identification Credential Program to PreCheck, to aviation worker programs. Aviation workers, themselves, are a diverse group of people who play many different and important roles within the commercial airport environment, from the person who works at the newsstand beyond the security checkpoints to the mechanic who has access to the plane itself to perform his or her duties. What these two people have in common is that they both go to work every day beyond the checkpoints in the secure area of the airport. We have to do everything within our power to ensure that people who go to work in these secure areas are exhaustively vetted, both before employment and on a recurring basis, and prove themselves to be trustworthy.

Last week, the Department of Homeland Security Office of Inspector General issued a report that detailed how 73 individuals with links to terrorism were able to get jobs with airlines and airport vendors and were cleared to access secure areas. That is unacceptable. First, we should all be grateful to the inspector general for bringing this to our attention. To know that this threat was out there, to think about what could have happened should be all the motivation we need to work together, act swiftly, and do what needs to be done to make sure this doesn't happen again.

That is why we are here today, not to create a spectacle or cast blame. We are here to figure out how this happened, what we need to learn from it, and what we need to do to close this gap in our security. I also want to point out that Inspector General Roth, himself, noted that TSA's vetting process was, "generally effective." So that is not the problem here. As far as I understand, there seem to be two main factors that allowed this to happen.

No. 1, because of the current interagency watch list policy, TSA doesn't have access to databases that would have captured the individuals in question and alerted TSA to their terrorism indicators. That, too, is simply unacceptable and has to change. TSA should have had access to all information about these individuals. TSA should have access to any and all information that will make their vetting process as exhaustive as possible.

No. 2, the report also made it clear that TSA's own databases are a mess. Eighty-seven thousand employee files without Social Security numbers, many with no passport number or proof of citizenship, 300 files with no full name for the employee. There is no excuse for that. It strikes me, as I am sure everyone, as sloppy. There is no place for sloppiness when we are dealing with the security of our Nation's aviation system.

We strive for a security system that is airtight and precise. In order to achieve that, our information must be airtight. Everything we do must be precise. The inspector general's office has issued six recommendations, all of which will help to address these issues. I appreciate the fact that TSA has concurred with these recommendations and is already taking steps to implement them.



I look forward to hearing more about these issues and corrective actions today. After this hearing, I look forward to taking up legislation authored by myself and Chairman Katko that will codify recommendations from this report and from another OIG report that details the need for TSA to properly manage its airport screening equipment maintenance program.

I want to thank each one of our witnesses for being here today. I am eager to hear all of your testimony and have a productive conversation about how we can do a better job vetting aviation workers, how we can do a better job keeping airports secure, and primarily keeping passengers safe.

Mr. Chairman, I thank you again for convening this hearing. I yield back the balance of my time.

Mr. KATKO. Thank you, Miss Rice.

I know at least the Chairman of the Homeland Security full committee, Mr. McCaul, plans on coming here and making a statement. When he comes, we will give him an opportunity to do so. He is held up in another hearing. I will extend the same courtesy to Mr. Thompson if he shows up.

With respect to the other Members of the committee, I want to remind you that opening statements may be submitted for the record. We are pleased to have several distinguished witnesses before us today on this important topic. Let me remind the witnesses that their entire written statements will appear in our record.

Somebody that is well familiar to this committee and to Homeland Security as a whole is Mr. Roth. Welcome back. Thank you for your continuing good work, sir. Ms. Fitzmaurice, of TSA, thank you for being here. Ms. Grover, thank you for being here as well. I would like to hear from Mr. Roth with respect to his opening statement.

**STATEMENT OF HONORABLE JOHN ROTH, INSPECTOR  
GENERAL, U.S. DEPARTMENT OF HOMELAND SECURITY**

Mr. ROTH. Chairman Katko, Ranking Member Rice, and Members of the subcommittee, thank you for inviting me here today to discuss the results of our most recent TSA audit.

Federal regulations require that individuals who work in secure areas of commercial airports undergo background checks. TSA and the airports are required to perform these checks before 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, and evidence of the applicant's authorization to work in the United States. The airports themselves collect this information used for vetting and submit it to TSA through a contractor.

Once TSA receives biographic data, it electronically matches it against an extract of the Terrorist Screening Database to identify individuals with potential links to terrorism. TSA also recurrently vets airport workers every time it receives a watch list update. Based on this review, TSA may direct the airport to grant, deny, or revoke a credential after coordination with other Government entities.

We found that TSA was generally effective in identifying individuals with links to terrorism. However, we did uncover a significant weakness. At our request, the National Counterterrorism Center performed a data match of over 900,000 airport workers who have access to secure areas against the National Counterterrorism Center's TIDE database. As a result of this match, we identified 73 individuals with terrorism-related category codes within the TIDE database who also had active airport credentials.

According to TSA officials, current interagency policy prevents TSA from receiving all terrorism-related codes during vetting. This lack of access to complete records resulted in TSA not discovering the issue with these 73 individuals. TSA officials candidly recognize 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 those categories.

In 2014, the TSA administrator authorized his staff to request some of the missing category codes for vetting. However, according to an official at the DHS Office of Policy, TSA and DHS has yet to formalize the request to the watchlisting interagency policy committee in order to receive additional categories of terrorism-related records.

Additionally, we found an issue with the manner in which airport workers are checked for criminal histories. The airports themselves maintain the ultimate authority to review and determine whether an individual's criminal history contains disqualifying crimes under Federal law. However, TSA did not have an adequate monitoring process in place to ensure that airport operators properly adjudicated these criminal histories.

TSA officials informed us that airport officials rarely or almost never documented the results of their criminal history reviews electronically. Without sufficient documentation, TSA cannot systematically determine whether individuals with access to secure areas of the airport are free of disqualifying criminal convictions. Moreover, under current law and FBI policy, TSA and the airports are not legally authorized to conduct recurrent vetting of criminal histories. We also found a weakness in the verification process for an individual's authorization to work in the United States.

As with criminal histories, it is the airport operators who are required to ensure that aviation workers are authorized to work before sending their information to TSA for review. TSA then verifies that aviation workers have lawful status. However, a review of TSA data showed that TSA has had to deny credentials for over 4,800 applicants because TSA determined that they did not prove their lawful status in the United States even after appeal. Now, this occurred despite the fact that these individuals had previously been cleared to work by the airports as being legally authorized to work.

Finally, we looked at the quality of the data that is involved in worker vetting. TSA relies on airports to submit complete and accurate aviation worker data. However, we identified thousands of aviation worker records that appeared to have incomplete or inaccurate biographic information. We made six recommendations in our report. TSA agreed to all the recommendations and provided

target completion dates for corrective actions. We will follow up on the implementation of these corrective actions.

Mr. Chairman, thank you again for inviting me to testify here today. I look forward to any questions you or other Members of the committee may have.

[The prepared statement of Mr. Roth follows:]

PREPARED STATEMENT OF JOHN ROTH

JUNE 16, 2015

Chairman Katko, Ranking Member Rice, and Members of the subcommittee: Thank you for inviting me here today 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.<sup>1</sup> We also reported on TSA worker vetting operations in 2011 and prior years.<sup>2</sup> 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.<sup>3</sup>

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 recently on multiple transportation security vulnerabilities that we believe TSA needs to address. Since 2004, we have published more than 115 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 is 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, 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 watch list update. TSA identifies potential matches to terrorism-related information using varied pieces of data such as names, 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

<sup>1</sup> *TSA Can Improve Aviation Worker Vetting (Redacted)*, OIG-15-98.

<sup>2</sup> *TSA's Oversight of the Airport Badging Process Needs Improvement*, OIG-11-95; *Transportation Security Administration's Aviation Channeling Services Provider Project*, OIG-13-42.

<sup>3</sup> *Covert Testing of Access Controls to Secured Airport Areas*, OIG-12-26.

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.

## 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 watch list.

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.<sup>4</sup> 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, current interagency policy prevents the agency from receiving all terrorism-related codes during vetting.

TSA officials recognize 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 must work with DHS to formalize a request to the Watchlisting Interagency Policy Committee in order to receive additional categories of terrorism-related records.

### *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. However, under current law and FBI policy, TSA and the airports are not legally authorized to conduct recurrent criminal history vetting, except for the U.S. Marshals Service Wants and Warrants database. This is because 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. TSA is planning this pilot program for multiple airports in late 2015.

### *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

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

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 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 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 1 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.

#### *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. Pursuant to the Privacy Act, TSA is not authorized to require the collection of SSNs.
- 1,500 records in TSA's screening gateway had individuals' first names containing two or fewer characters.
- Over 300 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 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 birth dates show that they were 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 will become effective for new or reissued badges, which should happen within 2 years as required by TSA's security policy.

#### RECOMMENDATIONS

We made six recommendations in our report:

- Follow up on the request for additional categories of terrorism-related records.
- Require inspectors to view original identity documents supporting airport adjudication of an applicant's criminal history and work authorization.
- Pilot FBI's Rap Back Program and take steps to institute recurrent vetting of criminal histories at all commercial airports.

- Require airports to link credential end dates to temporary work authorization end dates.
- Perform analysis to identify airports with weaknesses related to applicants' lawful status.
- Implement data quality checks to ensure complete and accurate data as required by TSA policy.

TSA agreed to all recommendations and provided target completion dates for corrective actions. DHS will follow up on implementation of these corrective actions.

#### 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 legislation pending in the House, 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.

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.

Mr. KATKO. Thank you, Mr. Roth, for your continued professionalism in handling these matters. We appreciate you being here today of course.

Our second witness, Ms. Fitzmaurice, the deputy assistant administrator for TSA's Office of Intelligence and Analysis. Prior to her current role, Ms. Fitzmaurice served as division director for the Checkpoint Solutions and Integrity Division within TSA's Office of Security Capabilities. In this position, she led TSA's efforts to identify, acquire, and manage state-of-the-art technologies and capabilities that screen passengers at U.S. airports. Prior to beginning her Federal career, Ms. Fitzmaurice held management positions with Airline Reporting Corporation, U.S. Airways, and Trans State Airlines. The Chair now recognizes Ms. Fitzmaurice to testify.

#### **STATEMENT OF STACEY FITZMAURICE, DEPUTY ASSISTANT ADMINISTRATOR, OFFICE OF INTELLIGENCE AND ANALYSIS, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY**

Ms. FITZMAURICE. Good morning, Chairman Katko, Ranking Member Rice, and distinguished Members of the subcommittee. I appreciate the opportunity to appear before you today to testify about TSA's aviation worker vetting program. TSA conducts security threat assessments for more than 2 million workers requiring bagged access to airports. These individuals undergo terrorist

watch list checks, as well as immigration status, and criminal history records checks.

TSA checks against the Terrorist Screening Database are constant and give us near-real-time notification of any changes to the list of known or suspected terrorists so that we can take appropriate action. Both the IG and an independent review of DHS's vetting processes deemed TSA's vetting to be effective. TSA has made key enhancements to aviation worker vetting through projects that began in 2012. These include the ability for airports to upload immigration and identity documents, to conduct more robust identity verification and immigration checks, and implementing system logic to reject inaccurate information. We will continue to work on improvements in this area.

Airport operators are responsible for reviewing FBI criminal history records and ultimately making a determination about granting badges to workers that provide secure access to our Nation's airport according to TSA's requirements. An airport operator may not issue a badge if TSA deems the individual to be ineligible. Airports represent a critical layer of security by making risk-based decisions using TSA provided information and locally-derived information for the final badging decision.

TSA recognizes the value of conducting more frequent or recurrent criminal checks on workers to identify cases where there has been subsequent criminal activity. TSA's use of criminal history records checks is considered by the FBI to be for non-criminal justice purposes according to pre-9/11 law and regulations. As such, TSA has not had access to criminal checks that are available to law enforcement agencies. However, in September 2014, the FBI implemented a new automated capability called Rap Back that will provide this service to other agencies such as TSA for a fee.

TSA and the FBI have been working together to implement recurrent criminal checks. TSA is planning for an initial Rap Back pilot in the aviation sector to begin later this calendar year. The IG recently made several key recommendations on worker vetting, including one that TSA had also identified as an area for enhancement in 2014. Namely, that there is additional intelligence-related data that may provide value and inform TSA's vetting decisions. Using this data, the IG identified 73 cases for additional attention.

To be clear, these individuals are not considered to be known or suspected terrorists. TSA has re-reviewed all 73 cases and found the individuals do not pose a threat to transportation security. The additional data did not change its original determination for these cases. These additional intelligence records do not meet the reasonable suspicion standard of being considered a known or suspected terrorist by the U.S. Government. That being said, TSA recognizes the value of having as much relevant data as possible to make informed decisions in its vetting. As such, former TSA Administrator Pistole signed a memo in 2014 supporting TSA's request and receipt for the additional data.

This information may not only be important for TSA to conduct its security threat assessment, but also may allow TSA to assist the intelligence and law enforcement community by identifying previously unknown associations of known or suspected terrorists. TSA and the Department are aggressively pursuing automated ac-

cess to the data and working to expedite the process in interagency coordination to complete the request. TSA concurs with all six of the IG recommendations and is taking steps to address all of them.

In addition to the three items I have already mentioned, we will also be including a requirement for inspectors to include verifying an airport badging office's review of applicant criminal history records and legal status, publishing guidance to all regulated airports to ensure that the airport badging offices deactivate the badges promptly when an individual's temporary authorization to work in the United States ends, and working with airports to analyze denials based on legal status, validate the reasons for the denial, and issue guidance to airports to address any weaknesses.

The IG findings support our efforts to improve the vetting of regulated aviation workers and compliment the steps TSA has taken to address the potential insider threat vulnerability at U.S. airports. We recognize the value of complete and accurate information when conducting vetting. We will continue to identify areas for improvements.

TSA appreciates the work of the IG during the course of this audit. We will use the information to enhance our processes going forward. I want to thank the committee for your interest in this important issue. I look forward to answering your questions.

Mr. KATKO. Thank you, Ms. Fitzmaurice, for your testimony.

Our third witness is Ms. Jenny Grover, director of the Homeland Security and Justice Team at the Government Accountability Office. Her portfolio includes GAO reviews of TSA and Coast Guard programs and operations. Ms. Grover joined the GAO in 1991. The Chair now recognizes her to testify.

**STATEMENT OF JENNIFER A. GROVER, DIRECTOR, TRANSPORTATION SECURITY AND COAST GUARD ISSUES, HOMELAND SECURITY AND JUSTICE TEAM, U.S. GOVERNMENT ACCOUNTABILITY OFFICE**

Ms. GROVER. Good morning, Chairman Katko, Ranking Member Rice, Chairman McCaul, and other Members and staff. I am pleased to be here today to discuss TSA's implementation and oversight of the aviation worker program which TSA and airports use to determine whether airport workers pose security threats.

TSA, in collaboration with airport operators and the FBI, completes applicant background checks, known as security threat assessments, for airport facility workers, retail employees, and airline employees. In general, security threat assessments include checks of an applicant's criminal history, immigration status, and known links to terrorism. TSA and airport operators have different responsibilities within the process.

Airport operators collect applicant information and send it to TSA for the security threat assessment. TSA reviews the results of the terrorism and immigration checks to determine if the applicant meets the eligibility criteria for holding an airport credential. TSA transmits the results of the FBI criminal history check, which contains information from a National fingerprint and criminal history system, back to the airport operator for review. Based on this information, the airport operator evaluates the criminal history to identify potentially disqualifying criminal offenses and then makes a



determination of eligibility. The airport also enrolls approved applicants and issues a credential providing for access to secured areas of the airport.

TSA has faced long-time challenges obtaining the necessary criminal history information to accurately assess aviation workers. In December 2011, we found that limitations in the criminal history checks increased the risk that the agency was not detecting all applicants with potentially disqualifying criminal offenses. For the purposes of accessing FBI criminal history records, TSA is considered a non-criminal justice requester, similar to that of a private company conducting an employment check on a new applicant. As a result, the information that TSA received on aviation work applicants was often incomplete.

For example, at the time of our report, TSA did not have access to many State records with information on sentencing, release date, and parole or probation violations. We recommended that TSA and the FBI jointly assess the extent to which this limitation posed a security risk and consider alternatives. TSA and the FBI concluded that the risk of incomplete information could be mitigated through improved access to State-supplied records. The FBI has since reported expanding the criminal history information that is available to TSA for these security threat assessments.

Our remaining vulnerability, as others have noted this morning, is that until recently, TSA did not conduct periodic criminal history checks of airport workers after they had been hired. In fact, workers who maintained continuous employment with the same airport authority did not undergo any subsequent criminal history checks.

In April 2015, TSA changed this policy by requiring periodic criminal history checks of all credentialed airport workers with unescorted access to secure areas of the airport. According to this requirement, TSA will conduct these checks until they are able to establish a system for real-time, recurrent criminal history checks, similar to the way that TSA conducts recurrent vetting against the terrorism database for their aviation workers.

In conclusion, with more complete and updated information about applicant and current worker criminal histories, TSA and airports are better positioned to detect all individuals with potentially disqualifying criminal offenses. TSA's new requirement to periodically conduct criminal history checks of their aviation workers is a positive interim step while TSA and the FBI work toward full implementation of the FBI's Rap Back service, which is intended to provide TSA and the airports with real-time criminal activity monitoring.

Chairman Katko, Ranking Member Rice, Chairman McCaul, this concludes my statement. I look forward to your questions.

[The prepared statement of Ms. Grover follows:]

PREPARED STATEMENT OF JENNIFER A. GROVER

JUNE 16, 2015

Chairman Katko, Ranking Member Rice, and Members of the subcommittee: I am pleased to be here today to discuss our past work examining the Transportation Security Administration's (TSA) Aviation Workers Program. It has been nearly 14 years since the attacks of September 11, 2001, exposed vulnerabilities in the Nation's civil aviation system. Since then, TSA, within the Department of Homeland Security (DHS), has taken steps to ensure that airport workers who require

unescorted access to secure areas of commercial (i.e., TSA-regulated) airports are properly vetted to identify those who may pose a security threat. These efforts are intended to reduce the probability of a successful terrorist or other criminal attack at the Nation's approximately 450 commercial airports. However, TSA has faced challenges in obtaining the necessary information to accurately assess aviation workers. According to TSA, the threat to civil aviation has not diminished—underscoring the need for effective airport worker screening programs.

As requested, my testimony today describes the role of TSA and airport operators in assessing aviation workers for potential security threats, as well as challenges and recent improvements. In carrying out this process, TSA and airports work in collaboration with the Federal Bureau of Investigation (FBI) to vet applicants against the FBI's criminal history records, terrorist watch lists and other databases, and issue credentials to qualifying airport facility workers, retail employees, and airline employees, among others. This statement is based on our report and testimonies issued from December 2011 through June 2015 related to TSA's efforts to vet aviation workers.<sup>1</sup> For our past work, we reviewed applicable laws, regulations, and policies as well as TSA program documents, decision memorandums, and other documents. We interviewed DHS, TSA, and FBI officials. We also conducted selected updates in June 2015 on recent DHS and TSA efforts to vet aviation workers. For these recent DHS and TSA efforts, we reviewed applicable policies and the Aviation Security Advisory Committee's (ASAC) April 2015 report on improving airport employee access control.<sup>2</sup> We reviewed the report's methodology and determined that the findings were reasonable for use in our report. Further details on the scope and methodology for the previously issued report and testimonies are available within each of the published products. We conducted the work on which this statement is based in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

#### BACKGROUND

In accordance with the Aviation and Transportation Security Act (ATSA), enacted following the September 11, 2001, terrorist attacks, TSA requires that airport operators (e.g., an airport authority) undertake specific actions before issuing credentials to airport workers seeking unescorted access to secure areas of an airport to reduce potential security risks posed by these workers.<sup>3</sup> For example, a worker seeking unescorted access to a Security Identification Display Area (SIDA) must first undergo a fingerprint-based criminal history record check.<sup>4</sup> TSA oversees implementation of these requirements through its Aviation Workers Program, which focuses on identifying security threats posed by those individuals seeking to obtain a credential for unescorted access to secure or restricted areas of airports. Specifically, TSA, in collaboration with airport operators and the FBI, completes applicant background checks, including Security Threat Assessments, for airport facility workers, retail employees, airline employees, and any other workers who apply for or are issued a credential for unescorted access to secure areas in U.S. airports. In general, Security Threat Assessments include checks for criminal history records and immigration status, checks against terrorism databases and watch lists, and checks for records indicating an adjudication of lack of mental capacity, among other things.

<sup>1</sup>See GAO, *Transportation Security: Actions Needed to Address Limitations in TSA's Transportation Worker Security Threat Assessments and Growing Workload*, GAO-12-60 (Washington, DC: Dec. 8, 2011); *Aviation Security: TSA Has Taken Steps to Improve Oversight of Key Programs, but Additional Actions Are Needed*, GAO-15-559T (Washington, DC: May 13, 2015); and *Aviation Security: TSA Has Taken Steps to Improve Oversight of Key Programs, but Additional Actions Are Needed*, GAO-15-678T (Washington, DC: June 9, 2015).

<sup>2</sup>See ASAC, *Final Report of the Aviation Security Advisory Committee's Working Group on Airport Access Control* (Arlington, VA: April 8, 2015).

<sup>3</sup>See generally 49 C.F.R. pt. 1542, subpt. C. In general, secure areas of the airport include areas specified in an airport's security program: (1) Where air carriers enplane and deplane passengers, sort and load baggage, and any adjacent areas (secured areas), (2) in which appropriate identification must be worn (SIDAs), (3) that provide passengers access to boarding aircraft and to which access is general controlled through the screening of persons and property (sterile areas), and (4) that include aircraft movement areas, aircraft parking areas, loading ramps, and safety areas that are not separated by adequate security systems, measures, or procedures (air operations areas). See 49 C.F.R. § 1540.5.

<sup>4</sup>See 49 C.F.R. § 1542.205.

## TSA AND AIRPORT OPERATORS SHARE RESPONSIBILITIES FOR AVIATION WORKER VETTING

TSA and airport operators each have certain responsibilities within the credentialing process. For example, we reported in December 2011 that airport operators are responsible for ensuring the collection of application information, transmitting the results to TSA for the Security Threat Assessment, enrolling approved applicants, and issuing credentials.<sup>5</sup> TSA's roles include adjudicating the immigration and terrorism checks, running automated FBI criminal history records, and transmitting the results of the criminal history record checks to the airport operators. The FBI's criminal history records contain information from a National fingerprint and criminal history system.<sup>6</sup> If an individual has a criminal record in the database, the FBI provides the criminal history record check results to TSA. TSA, in turn transmits the results to the airport operator. The airport operators are responsible under TSA regulations for adjudicating the criminal history to identify potentially disqualifying criminal offenses specified under TSA regulations, and making a final determination of eligibility for a credential.<sup>7</sup> In doing so, airport operators may follow up with an applicant if the FBI Record of Arrests and Prosecutions (RAP) sheet TSA provided lacks a disposition of a criminal offense—which is necessary for the airport operators to determine if the applicant has potentially disqualifying criminal offenses.<sup>8</sup> Furthermore, airport operators, and not TSA, are the entities responsible for revoking the issued credentials.<sup>9</sup> For example, airport operators are to revoke a worker's credentials if TSA determines the worker poses a threat or violates airport security policy. Figure 1 summarizes the credentialing processes and respective responsibilities of TSA and airport operators under TSA's Aviation Workers Program.

---

<sup>5</sup>GAO-12-60.







<sup>6</sup>The system provides automated fingerprint search capabilities, latent search capability, electronic image storage, and electronic exchange of fingerprints and responses. A segment of this system is the FBI-maintained criminal history record repository, known as the Interstate Identification Index (III, or Triple I) system that contains records from all States and territories, as well as from Federal and international criminal justice agencies. The State records in the III are submitted to the FBI by central criminal record repositories that aggregate criminal records submitted by most or all of the local criminal justice agencies in their jurisdictions. The FBI's criminal history records check is a negative identification check, whereby the fingerprints are used to confirm that the associated individual is not identified as having a criminal record in the database.

<sup>7</sup>See, e.g., 49 C.F.R. § 1542.209.

<sup>8</sup>See appendix I for a list of TSA Aviation Worker disqualifying criminal offenses.

<sup>9</sup>If TSA determines that an individual poses a threat based on checks of information in the Terrorist Screening Database or immigration checks, TSA will notify the airport operator to revoke the credential.

**Figure 1: Summary of Credentialing Processes and Responsibilities for TSA and Airport Operators under TSA's Aviation Workers Program**

Transportation Security Administration (TSA) and airport operator credentialing responsibilities under TSA Aviation Worker Program	
TSA	Airport operator
<b>Enrollment</b> 	Applicant provides biographic and biometric information to airport operator. Airport operator submits information to TSA.
<b>Background check</b> 	TSA vets and adjudicates terrorist and immigration information, and provides results of criminal history checks to airport operator.  Airport operator adjudicates criminal history and makes determination of eligibility.
<b>Issuance</b> 	Airport operator issues access badge to employee.
<b>Verification</b> 	Airport operators responsible for implementing access control system as part of TSA-approved security plan.
<b>Renewal</b> 	In April 2015, TSA modified existing requirements to address the need for recurrent criminal history checks.  As part of the renewal process, the expiring badge must be retrieved by the airport operator.
<b>Revocation</b> 	Airport operators can revoke a badge if an individual is no longer employed by airport employer, or if an airport is informed by TSA of derogatory information related to immigration status or during recurring criminal history records or recurring terrorist screening checks.

Source: GAO analysis of Department of Homeland Security information; Art Explosion (clip art) | GAO-15-704T

**TSA HAS TAKEN ACTIONS TO ADDRESS LIMITATIONS IN AVIATION WORKER VETTING**

Criminal history record checks are a key element of the Security Threat Assessment process for TSA's Aviation Worker Program, helping to ensure that the agency and airport operators detect those applicants with potentially disqualifying criminal offenses. However, TSA has faced challenges in ensuring it has the necessary criminal information to effectively conduct Security Threat Assessments for applicants to its Aviation Workers Program. In December 2011, we found that, according to TSA, limitations in its criminal history checks increased the risk that the agency was not detecting potentially disqualifying criminal offenses as part of its Security Threat Assessments for airport workers.<sup>10</sup> Specifically, we found that TSA's level of access to criminal history record information in the FBI's Interstate Identification Index excluded access to many State records such as information regarding sentencing, re-

<sup>10</sup>GAO-12-60.

lease dates, and probation or parole violations, among others. For the purposes of accessing criminal history records, FBI provided TSA the level of a noncriminal justice requestor (e.g., equal to that of a private company conducting an employment check on a new applicant, according to TSA). As a result, TSA reported that its access to and airports' ability to review applicant criminal history records was often incomplete. We found that TSA and the FBI had not assessed whether a potential security risk in TSA's Security Threat Assessment process existed with the level of access to FBI criminal records that TSA had at the time.

We recommended that the TSA and the FBI jointly assess the extent to which this limitation may pose a security risk, identify alternatives to address any risks, and assess the costs and benefits of pursuing each alternative. In May 2015 and June 2015, we reported that TSA and the FBI have since taken steps to address this recommendation. For example, in 2014, the agencies concluded that the risk of incomplete information did exist and could be mitigated through expanded access to State-supplied records.<sup>11</sup> TSA officials reported that the FBI has since taken steps to expand the criminal history record information available to TSA when conducting its Security Threat Assessments for airport workers and others. For example, TSA reported that the study between the FBI and TSA culminated in the FBI implementing system changes to provide the TSA with access to expanded criminal history record information. According to TSA officials, the FBI's release of its Next Generation Identification System—which the FBI reported achieving full operational capability in September 2014—has been enhanced to expand the State-provided criminal history records that are now incorporated into all FBI criminal history record information for TSA's Security Threat Assessments for aviation workers.<sup>12</sup> We have not evaluated TSA's use of the new system.

Further, in April 2015, TSA updated existing requirements to address the need for recurrent criminal history records checks for credentialed airport workers with unescorted access to secure airport areas at periodic intervals. Until recently, TSA did not require periodic criminal history checks of workers with unescorted access authority as long as workers maintain continuous employment with the same issuing authority. TSA updated its requirements in response to the ASAC's recommendation and the Secretary of DHS's statement regarding airport security enhancements.<sup>13</sup> ASAC recommended that TSA should incorporate real-time criminal activity monitoring into the aviation worker vetting process in its final report on improving airport employee access control. ASAC found that TSA's practice of reviewing criminal history records once—at the time of vetting for initial employment—created the potential for TSA and airport operators to be unaware of aviation workers who had subsequently engaged in potentially disqualifying criminal activity yet continued to hold active credentials. ASAC reported that real-time criminal activity monitoring should be a part of the vetting process, similar to the perpetual vetting of aviation workers conducted by TSA against terrorist watch lists. Specifically, ASAC recommended that TSA accelerate implementation of a pilot of criminal activity monitoring using FBI's Rap Back Service, with a goal of full implementation of the service by the end of 2015.<sup>14</sup> The Secretary of DHS stated that until TSA establishes a system for real-time recurrent criminal history records checks for all aviation workers, TSA should require fingerprint-based criminal history records checks periodically for all airport employee SIDA badge-holders.

Chairman Katko, Ranking Member Rice, and Members of the subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

<sup>11</sup> GAO-15-559T and GAO-15-678T.

<sup>12</sup> According to the FBI, the Next Generation Identification System is an incremental replacement of a previous fingerprint identification system that provides new functionality and improves existing capabilities. The technological upgrade accommodates increased information processing and sharing demands from local, State, Tribal, Federal, and international agencies.

<sup>13</sup> ASAC, at the request of TSA in January 2015, created a working group comprised of representatives from the aviation industry tasked with analyzing the adequacy of existing security measures and recommending any additional measures needed to improve employee access controls. See 49 U.S.C. § 44946 (requiring establishment of an ASAC within TSA to provide advice and recommendations on aviation security matters, including the development, refinement, and implementation of policies, programs, rulemaking, and security directives pertaining to aviation security, while adhering to sensitive security guidelines).

<sup>14</sup> FBI introduced its Rap Back Service in September 2014 as part of its Next Generation Identification System. According to the FBI, the Rap Back Service provides users, such as airport authorities, the capability to receive immediate notification of criminal and, in limited cases, civil activity of enrolled individuals that occur after the initial processing and retention of criminal or civil fingerprint transactions, such as the fingerprint-based criminal history records checks currently conducted by TSA and airport operators.

APPENDIX I: CRIMINAL OFFENSES THAT DISQUALIFY APPLICANTS UNDER THE AVIATION WORKERS PROGRAM FROM ACQUIRING AN AIRPORT-ISSUED BADGE

In accordance with 49 C.F.R. §§ 1542.209, 1544.229, and 1544.230, an individual has a disqualifying criminal offense if the individual has been convicted, or found not guilty of by reason of insanity, of any of the crimes listed below in any jurisdiction during the 10 years before the date of the individual's application for unescorted access authority, or while the individual has unescorted access authority.

DISQUALIFYING CRIMINAL OFFENSES

1. Forgery of certificates, false marking of aircraft, and other aircraft registration violation; 49 U.S.C. § 46306.
2. Interference with air navigation; 49 U.S.C. § 46308.
3. Improper transportation of a hazardous material; 49 U.S.C. § 46312.
4. Aircraft piracy; 49 U.S.C. § 46502.
5. Interference with flight crew members or flight attendants; 49 U.S.C. § 46504.
6. Commission of certain crimes aboard aircraft in flight; 49 U.S.C. § 46506.
7. Carrying a weapon or explosive aboard aircraft; 49 U.S.C. § 46505.
8. Conveying false information and threats; 49 U.S.C. § 46507.
9. Aircraft piracy outside the special aircraft jurisdiction of the United States; 49 U.S.C. § 46502(b).
10. Lighting violations involving transporting controlled substances; 49 U.S.C. § 46315.
11. Unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers contrary to established security requirements; 49 U.S.C. § 46314.
12. Destruction of an aircraft or aircraft facility; 18 U.S.C. § 32.
13. Murder.
14. Assault with intent to murder.
15. Espionage.
16. Sedition.
17. Kidnapping or hostage taking.
18. Treason.
19. Rape or aggravated sexual abuse.
20. Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon.
21. Extortion.
22. Armed or felony unarmed robbery.
23. Distribution of, or intent to distribute, a controlled substance.
24. Felony arson.
25. Felony involving a threat.
26. Felony involving—
  - (i) Willful destruction of property;
  - (ii) Importation or manufacture of a controlled substance;
  - (iii) Burglary;
  - (iv) Theft;
  - (v) Dishonesty, fraud, or misrepresentation;
  - (vi) Possession or distribution of stolen property;
  - (vii) Aggravated assault;
  - (viii) Bribery; or
  - (ix) Illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than 1 year.
27. Violence at international airports; 18 U.S.C. § 37.
28. Conspiracy or attempt to commit any of the criminal acts listed above.

Mr. KATKO. Thank you, Ms. Grover.

The Chair now recognizes the Chairman of the full Homeland Security Committee, the gentleman from Texas, Mr. McCaul, for any statement he may have.

Mr. MCCAUL. I would like thank Chairman Katko and Ranking Member Rice for holding this important hearing.

Recent reports about the TSA screening, in my view, are deeply disturbing and call into question some of the post-9/11 security measures we have worked hard to put in place. Yet 14 years after that horrible day, Islamist terrorists are still plotting daily to kill Americans. Lately, the threat picture has gotten worse.

Our aviation sector is of particular interest to the terrorists. They think that by taking down airplanes, they can bring down our economy. Last week we reportedly hit al-Qaeda's No. 2 in a drone strike in Yemen, where the terror group has been focused for years on developing bombs to plant on airplanes. It was an important counterterrorism victory. But it won't stop terrorists from aiming their sights at our skies.

As we stare down these threats, Congress and the American people need confidence in our defenses. Terrorists have to be right only once. To defend ourselves, we have to be right 100 percent of the time. Millions of travelers pass through our Nation's airports every year. We need to know that the systems in place will protect them. But in recent weeks, TSA has given us more concern than confidence.

Reports about TSA's performance have alarmed the American people and raised fears that bombs could pass through airport passenger screening and terrorists might slip through TSA's employee vetting. We need to get to the bottom of these claims and do everything possible to deny terrorists an opportunity to exploit our defenses.

Next month, I plan to hold a hearing on aviation security with the new TSA administrator once he is confirmed. I want him to outline his vision for TSA and give us answers on how he will close any identified vulnerabilities. This will not be easy. But in order to win the confidence of the American people, TSA needs a good wire brushing and strong leadership.

We cannot become complacent about the threat. We can and must improve our screening capabilities. We need aviation workers who are thoroughly vetted. As the first step to tackle these challenges, I am co-sponsoring H.R. 2750, the Improved Security Vetting for Aviation Workers Act, introduced by Chairman Katko, which codifies the inspector general's six recommendations to ensure there are no loopholes in the security background checks for aviation workers.

I also strongly support H.R. 2770, the Keeping Our Travelers Safe and Secure Act, introduced by Ranking Member Rice, which would close additional screening gaps and strengthen our aviation security. I want to thank the DHS Inspector General Roth for his leadership and strong oversight at TSA and DHS in bringing these vulnerabilities to our attention. I also want to thank the TSA and GAO witnesses here. I hope they are committed to changing the agency's direction and restoring the trust of the American people.

When I heard that 73 airport workers had ties to terrorism, when I got that news, well, first of all, I couldn't believe it, and I want additional briefings on these ties to terrorism, but that is totally unacceptable 14 years after 9/11. I think the American people deserve better. When we see, you know, the grandma, the veteran, the Active-Duty service, the children being patted down at these airports and water bottles being taken out of luggage and all this going on. Yet, 96 percent of the stuff gets through. We can't talk about what it is because it is Classified. But 96, that is a 4 percent success rate.

The American people deserve better. They deserve to feel safe when they travel on airplanes. With that, Mr. Chairman, I yield back.

Mr. KATKO. Thank you very much, Chairman McCaul.

I now recognize myself for 5 minutes to ask questions. I will start with Mr. Roth. Briefly summarizing your findings in your report and the recommendations, you recommend basically four broad categories of recommendations. I just want to make sure I got them right here. No. 1, TSA should request and review additional watch list data, is that correct?

Mr. ROTH. That is correct.

Mr. KATKO. No. 2, that they require that airports improve verification of applicants' rights to work, correct?

Mr. ROTH. Correct.

Mr. KATKO. No. 3, that they revoke credentials when the right to work expires?

Mr. ROTH. Correct.

Mr. KATKO. No. 4, to improve the quality of vetting data, is that correct?

Mr. ROTH. Yes, sir.

Mr. KATKO. All right. Ms. Fitzmaurice, does TSA agree with all those recommendations?

Ms. FITZMAURICE. Yes. They do.

Mr. KATKO. All right. I want to focus on requesting and reviewing additional watch list data first. I will start with Mr. Roth briefly. Could you tell me, you mentioned during your testimony that about 900,000 individuals, employees Nation-wide were run through that National Counterterrorism Center's TIDE database, is that correct?

Mr. ROTH. Yes, sir.

Mr. KATKO. All right. How onerous a task was it to do that?

Mr. ROTH. Well, for us it was actually, the actual task of running it, and actually NCTC did it for us, the legal authorization for it took some time. We had to get a memorandum of understanding between TSA and NCTC to do it.

It took about 18 months to get all the legal authorizations that we needed to do it because of the requirements of the Data Matching Act. So legally and bureaucratically it was a huge lift. But then actually to do the match was quite easy.

Mr. KATKO. Okay. So the mechanical of checking against a database, once those hurdles are cleared, is relatively easy?

Mr. ROTH. Yes. The size of the data is not that large. So it was not that big of a task to match one set of data against the other set of data.

Mr. KATKO. So if we can fix these hurdles, it should be a relatively easy task to have this vetting going through the database on a regular basis?

Mr. ROTH. Yes, sir.

Mr. KATKO. All right. Thank you. Ms. Fitzmaurice, a couple questions for you. I would like to know when TSA first became aware of this problem with respect to not getting appropriate codes to run names through the database.



I know from at least May 2014, there was a memo to Administrator Pistole advising that they needed additional codes from TIDE for employee screening, is that correct?

Ms. FITZMAURICE. That is correct.

Mr. KATKO. All right. To your knowledge, is that when the administrator first became aware of this being a problem?

Ms. FITZMAURICE. That is my understanding.

Mr. KATKO. Okay. So May 2014, at least, the administrator, the head of TSA was aware of the fact that they may not be, they were getting incomplete data regarding employees and that that may affect whether individuals with terrorist ties are working at airports across this country, is that right?

Ms. FITZMAURICE. Yes. If I may explain the distinction of the information that we are requesting, TSA receives watch-listed information that is maintained by the FBI's Terrorist Screening Center. That information is the information that we primarily use in our vetting process. That is who the Federal Government has deemed to be known or suspected terrorists and meets the reasonable suspicion standard, which is why that is then shared with us for the watchlisting purposes.

What we are seeking access to is additional intelligence-related information that is contained in the NCTC TIDE database. I think it is important to understand that the information that are on the watch list are in TIDE, but not everyone in TIDE is a terrorist and meets that reasonable suspicion standard to be then put on the watch lists.

Mr. KATKO. Understood. But the fact remains that there was at least 73 individuals that had potential ties to terrorism that were not identified because you did not have the appropriate information, is that correct?

Ms. FITZMAURICE. That is correct. We did not have access to that information. We are seeking that access. We did review, though, all of the cases of those 73 individuals, and have determined they do not pose a threat to transportation security.

Mr. KATKO. Who made that determination?

Ms. FITZMAURICE. TSA did, sir.

Mr. KATKO. Did anybody from outside TSA share in making that determination?

Ms. FITZMAURICE. So sir, as part of our typical process, when we look at information and we look at individuals who may have some nexus to terrorism, we oftentimes will consult with various law enforcement and intelligence community partners.

Mr. KATKO. Did you do that?

Ms. FITZMAURICE. We do that regularly as part of our process.

Mr. KATKO. So the question is clear, with respect to these 73 individuals that have potential ties to terrorism according to the TIDE database, TSA has made their own independent determination that they don't pose a threat?

Ms. FITZMAURICE. TSA reviewed all of the 73 records on these individuals, determined that they did not pose a threat to transportation. That is part of TSA's kind of day-in and day-out process. But every time we understand that someone may have a potential nexus, they may not be designated as a known or suspected ter-

rorist, we do do that consultation with the IC and other law enforcement—

Mr. KATKO. I just want to make sure you are answering the question. Just a brief yes or no. Did you consult with people outside of TSA before you made the ultimate determination that these 73 individuals who are on the TIDE database don't pose any threat to TSA? Did you consult with outside people, yes or no?

Ms. FITZMAURICE. Yes. That is part of our process. We did.

Mr. KATKO. Okay. Okay. I take it that is something we can see in a secured setting, the information regarding that?

Ms. FITZMAURICE. Yes. We would be happy to share that in a closed setting.

Mr. KATKO. More importantly, this has raised a concern, of course, about a gap in, the biggest concern I have is the amount of time it takes, once a concern is raised with TSA, until the time when TSA actually acts upon it. So I guess from a guideline standpoint, we have May 2014 is when the information was brought to Administrator Pistole, correct?

Ms. FITZMAURICE. Yes, sir.

Mr. KATKO. What did TSA do after that to try and fix this problem? Okay, I know as of today, a year later, the problem has not been fixed. So tell us what you have been doing in the mean time?

Ms. FITZMAURICE. Certainly. So yes, the administrator did sign a memorandum, May of last year, acknowledging our interest to receive access to this information. We have been engaged in on-going discussions in the interagency to receive access to this information.

I just recently came back to the Office of Intelligence and Analysis in March. Since my return to the office, have had numerous interagency discussions on this topic. We are working to expedite this process in our request to gain access to this information.

Mr. KATKO. With all due respect, when you say requesting to expedite this process, it has been a year, right? It has been a year. You realize that what could be a potentially serious security gap, an obvious security gap. It has been a year. That doesn't sound like it is being expedited.

Ms. FITZMAURICE. So, you know, I understand your point there. Like I said, we are working very hard to gain access to this information.

Mr. KATKO. When you say very hard, what does that mean?

Ms. FITZMAURICE. So we have been having—

Mr. KATKO. Because, you know, quite frankly, with respect to employee screening at airports, we have had this problem since 2011. We are still talking about problems with employee screening at airports 4 years later. We hear the same thing from TSA all the time, we are working on it. Well, with all due respect, and I know you are just the person here filling in for someone who is unavailable, but that is not acceptable.

You have the Nation's security in your hands, this agency does. To sit there and give us a bureaucratic response we are working on it in an expedited manner, you are talking about a gap in terrorist watch lists. You are saying you are working on it?

Ms. FITZMAURICE. So we are working on it. But I think what is really important to understand is that we do receive the Terrorist

Screening Database and those are the individuals that are deemed to be threats to transportation security.

We do vet all of the aviation workers against those. We have taken action on those. What we are seeking to do now is gain access to additional information that will assist us and provide a fuller context of who these individuals are and potentially identify unknown associations.

Mr. KATKO. The point is, and I ask you to take it back to your supervisors, and we are going to make the point crystal clear to them, and actually Mr. Rogers and I have made it clear to him again and again and so have many others here, the fact remains, TSA is not responding in a timely manner to seemingly very important issues.

As it stands right now, were it not for the IG report, I highly doubt that we would be any closer to getting access to the TIDE database because the TIDE database identified 73 people you didn't know about that may have had ties to terrorism. Your determination whether or not they have ties to terrorism is an internal thing that we will take a look at. But the bottom line is it needs to be more quickly done. We cannot have a bureaucratic morass in charge of guarding our airports. We just can't.

With that, I will yield back questioning to the Ranking Member, Miss Rice.

Miss RICE. Thank you, Mr. Chairman. Ms. Grover, you mentioned something in your testimony about how the TSA is not qualified as a law enforcement agency which limits the ability for them to get relevant information regarding someone's background. Is that a change that needs to be made to expand the databases that TSA would have access to to ensure that the vetting can be as thorough and complete as possible?

Ms. GROVER. So this has been a topic of discussion for many years. The Compact Act from 1998 is what set the requirements for requesters that were considered to be having criminal justice access versus non-criminal justice access.

When we did our work several years ago, TSA's position was that they didn't really fit neatly into either one of those categories. It was their position that the non-criminal justice access records wasn't meeting their needs, which it clearly was not because at the time they only had access to information from about 15 States and really didn't have the information that they needed to make a complete determination of eligibility.

They have worked with the FBI. In the past, the FBI has determined that they are not eligible for the different status of criminal justice requester and has expanded the database. So I believe now they have access to information from about 41 States. That certainly comes much closer to meeting their needs.

Miss RICE. Okay. But that is not going to be complete until they have access to all 50 and they are treated, for all intents and purposes, like a law enforcement agency. So we have to deal with that change. Okay. So you answered the second question I was going to ask.

Ms. Fitzmaurice, one of the first things that you said in your testimony was that the vetting process by the TSA has been found to be effective, whether that is Mr. Roth's finding or your finding. I

have got to tell you, just sitting here, how is it possible that anyone can come to that conclusion when we are talking about all of these deficiencies?

Ms. FITZMAURICE. No, I understand that. Let me provide some context for that comment. So, yes, the inspector general, as part of his report, did say they found our vetting processes to be generally effective. Additionally, several years back, the Department sponsored a review of DHS's vetting programs. We participated in that. The review of that found that TSA's system was actually, I think, one of the best performing in effective systems that DHS has in the vetting enterprise.

I think one of the key things that we have to keep in mind and part of what we are talking about today, though, is the information that we have access to. So we have a very sophisticated vetting system that takes millions of records and vets that against the databases of known and suspected terrorists. But we are absolutely dependent on having access to the right information about individuals who pose, you know, a threat to transportation security and who also may have some value from an intelligence standpoint.

Additionally, as has been highlighted, you know, the other piece that is important on the information that we receive on the applicants who are seeking to work in our transportation system. So we are focused on those areas right now. But what my comment was specifically referencing was the effectiveness of the system that we have built, this very complex vetting system.

Miss RICE. I think it is clear after today and probably clearer much earlier that we can't use that word effective at this point in my opinion.

Mr. Roth, I just want to ask you, you said that TSA denied credentials to 4,300 applicants who had previously been found to be okay? Can you just elaborate on that? Do you know what I am making reference to?

Mr. ROTH. With regard to immigration status?

Miss RICE. Yes. Yes. So how did that happen? If you can do it quickly because I have a couple other questions.

Mr. ROTH. Yes. That is precisely my question: How could this happen? I mean, the airports are legally responsible for ensuring immigration status, that these folks have lawful authority to work. They do that. By the time they send it to TSA, they are basically certifying that—

Miss RICE. They being who? Who sends that information?

Mr. ROTH. Sorry. The airport operators.

Miss RICE. The airport operators send the background information to TSA?

Mr. ROTH. With the certification that these folks, in fact, are legally entitled to work.

Miss RICE. So this is a deficiency on the part of the airport operator not doing—

Mr. ROTH. Correct. Then what TSA does is they take that information, they bounce it off of CIS records. That is where we found the discrepancy.

Miss RICE. Okay. So it is clear, I think, from what we are hearing here today that post, you know, 9/11, 14 years post-9/11, we still have Federal agencies and some private operators who are

siloing relevant information in a way that could lead to a catastrophe. How do we fix that, Mr. Roth?

Mr. ROTH. Well, certainly the airports themselves under law have the obligation to certify whether or not someone meets the criminal history check. In other words, they are void of any disqualifying criminal offenses.

That is 450 airports across the country. TSA is obligated to do a quality check on that. Unfortunately, because these aren't electronic records, they have to do a manual review. So if they do an airport inspection, they might do a manual review of, in the larger airports, only about 1 percent of the applications to determine whether or not the airport workers who have these SIDA badges, in fact, have disqualifying criminal offenses.

Miss RICE. Mr. Roth, I have got to tell you, I think that is one of the most disturbing things that I have heard here, that airport operators are not doing their due diligence to ensure that people that they are sending to you to get the stamp of approval, they are not giving you the relevant information that you need.

Mr. ROTH. I share your concern. It is especially concerning given the fact that, you know, there are no layers of security. Once you have a SIDA badge, that means you have unescorted access to anywhere in the airport. You can load baggage. You can have access to the aircraft. You can do basically anything unescorted. That, obviously, is concerning if we don't have a better understanding of who these airport workers are.

Miss RICE. Well, certainly the airport operators have to assume an enormous amount of accountability and responsibility. We have to figure out a better way to check to make sure that the information that they are giving to the TSA is correct.

Thank you, Mr. Roth and Ms. Fitzmaurice, and Ms. Grover. I yield back my time. Thank you, Mr. Chairman.

Mr. KATKO. Thank you, Miss Rice. The Chair now recognizes Mr. Rogers from Alabama for questions he may have.

Mr. ROGERS. Thank you, Mr. Chairman. Now, Mr. Roth, and this could be for Ms. Fitzmaurice, either one, because both of you have just made statements that inferred that you don't have access to databases that would give you the relevant information to make sure that these staffers don't get the SIDA badge, is that what I am hearing?

Ms. Fitzmaurice, let me go to you, you made reference a little while ago that you can't do your job without access to important information. So you are saying that you don't have that access?

Ms. FITZMAURICE. So we do have access to the U.S. Government's terrorist watch list data. What we are seeking access to is additional intelligence information on individuals. We are working through the interagency currently to request that.

Mr. ROGERS. Is that an existing database that you want access to?

Ms. FITZMAURICE. That is a database that we are seeking some automated access to be able to incorporate additional data into our automated vetting processes.

Mr. ROGERS. Heretofore, you have been told you cannot have access? Or is it just something you all hadn't thought of?

Ms. FITZMAURICE. I think that when we recognized the value of this, we have been working to pursue gaining access to this.

Mr. ROGERS. But you knew about it before now? I am trying to figure out why at this late time you are just now saying well, we probably should have had access to that database. If it was a database that had information about potential terrorists in it, why wouldn't you already be plugged into it?

Ms. FITZMAURICE. So again, I think what we have to understand is the watch lists, which are maintained by the FBI's Terrorist Screening Centers, are what are determined to be individuals who pose, you know, threats to transportation. We receive those watch lists for purposes of our vetting.

I think what we have recognized over time through our experience in vetting individuals and understanding the additional intelligence information that is contained in TIDE, we believe that we can supplement the value of what we do by identifying potentially individuals who may be unknown and——

Mr. ROGERS. Who has control of that database now?

Ms. FITZMAURICE. So that database that we are talking about is maintained by the NCTC.

Mr. ROGERS. Okay. Are they giving you any problems about accessing it? Is it just a technical issue now? Are they happy to let you in on it?

Ms. FITZMAURICE. Yeah. This is a coordination discussion right now with the interagency. The vetting systems are very complex. You know, we have the airports, we have the airlines, they are submitting information to us. We have our system that is actually doing the analysis. We are getting information from the watchlisting community. So it is really just more of the complexities of that interagency coordination process that we are working through.

Mr. ROGERS. How long do you think it will take you to work through that?

Ms. FITZMAURICE. I am very optimistic now. We have had frequent and on-going discussions on this matter. I would expect that we will be able to work through it in the very near future.

Mr. ROGERS. That is very lawyerly.

Ms. FITZMAURICE. I am not a lawyer, sir.

Mr. ROGERS. You sound like one.

Mr. KATKO. All right, just for the record, that hurts me because I am a lawyer.

Mr. ROGERS. I am a recovering attorney too. That is why I know one when I see one. So 60 days? Ninety days?

Ms. FITZMAURICE. I can tell you that we are having daily conversations on this topic. Even as frequent as this afternoon, we will be continuing those discussions on how we can seek and gain the access.

Mr. ROGERS. Mr. Roth, is what she just described what you were making reference to about the SIDA badges?

Mr. ROTH. Somewhat. It is a little more complicated than that from our point of view. There are a number of codes that we are talking about——

Mr. ROGERS. A number of what?

Mr. ROTH. Of codes or sort-of categories of individuals or names in the large TIDE database. Now, some of those are, in fact, known or suspected terrorists that TSA does not have access to. Then there are others that are out there that are simply in the large TIDE database that really aren't used for watchlisting purpose, although TSA would like them to be noted for watchlisting purposes.

So there is really two categories of information. Some that is already sort-of vetted information, for example, there are several of these categories that other components within DHS gets but TSA doesn't get.

Mr. ROGERS. Why?

Mr. ROTH. It is difficult to describe in an open setting. But we can certainly explain it later on if you would wish.

Mr. ROGERS. Yes, I do. Let me ask, is this the first time that you have done an IG report on this problem?

Mr. ROTH. We have done reports on access badges in general, control over access badges. This is the first time, though, that we have done sort-of a data run comparing the SIDA badges to the terrorist databases.

Mr. ROGERS. Okay. All right. Do you agree with Ms. Fitzmaurice's characterization that the 73 people that were identified as having terrorist ties really weren't a problem?

Mr. ROTH. We don't have any information as to the process that TSA used once we gave them those names in November of last year. I would say that the more information that you have, the better decisions that you make. So whether or not these 73 individuals, in fact, did not pose a threat to terrorism doesn't mean that the system is working perfectly.

Mr. ROGERS. Well, my time is up. I hope one of the other Members will pick up on this. Because I would like to know if they weren't a problem, why were they on the list to begin with? With that, I yield back. Thank you.

Mr. KATKO. Thank you, Mr. Rogers. The Chair now recognizes Mr. Payne from New Jersey for questioning.

Mr. PAYNE. Thank you, Mr. Chairman. Thank you to the Ranking Member of this committee. Mr. Roth, a bit of a kind-of confusing element in your most recent report is how TSA's vetting process can be considered generally effective, yet 73 individuals with links to terrorism were not found during this process. It seems a little contradictory. Can you elaborate?

Mr. ROTH. Certainly. Thank you for that opportunity. When we talk about generally effective, what we are talking about is the operation that the vetting unit does within TSA. You know, they are only as good as the information that they get. So they do a very significant job, for example, they have over 2.2 million recurring vetting hits that they have to process every year. That is about 6,000 per day.

Additionally, they have to actually manually review 24,000 records a year, so that is 2,000 records a month, 500 records a week, to, you know, look at potential hits off the Terrorist Screening Database, to see whether or not these, in fact, are the individuals who are listed on the database itself.

So, I mean, they do a good job with the information that they have. But, again, what we had said is that we uncovered a vulner-

ability which is they didn't have all the information they needed to do their job.

Mr. PAYNE. So basically with the volume, if it was other than an issue of terrorism, it would be considered not that bad. But, you know, the potential of 73 individuals, you only need one to have ill will against this country.

Mr. ROTH. That is the nature of the threat that TSA faces. It is an asymmetric threat, that all it takes is one. They have to be right every single time.

Mr. PAYNE. Your report acknowledges passport numbers and Social Security numbers being strong matching elements, yet neither is required during the application process. In your view, can TSA effectively identify potential risk if such elements are discounted?

Mr. ROTH. I think it makes their job more difficult. One of the things with regard, for example, the Social Security numbers, that is probably the best identifier you can use as far as an individual to being able to match an applicant off of the database. Unfortunately, the Privacy Act, which has some exemptions, does not exempt TSA from requiring SIDA badge applicants to have a Social Security number. That is something that I think would be a useful thing to have.

Mr. PAYNE. Okay. Ms. Fitzmaurice, during the Q and A with the Members up here, what leverage do we have with the airport operators if they are not complying and giving the information? You know, I believe you said that there is a lapse sometimes with the airport operators in doing that job. What leverage do we have to make sure that they are complying?

Ms. FITZMAURICE. So, you know, before we get to the compliance piece, I think what is important is us working closely with the airport operators to identify the areas for improvement, put out guidance on how we can do that, work with them to implement that, and then ensure that we have a robust compliance mechanism to go back and review and ensure that they are doing that, and, you know, take corrective action if we continue to find that they are not complying with that.

Mr. PAYNE. What would those corrective actions consist of? If we are having, you know, obviously continued issues around them getting to where we need them to be, what, what leverage do we have if they are falling short?

Ms. FITZMAURICE. Sure. Well, we do have formal security programs with all of the airports that they are required to comply with. We have inspectors who go out and review their performance against those requirements. I am not intimately familiar with all of the consequences, I will say, with respect to the, if there are issues of noncompliance, but happy to follow up with you on that.

Mr. PAYNE. Okay. Well, what can we do to strengthen the relationship TSA has with the airports to ensure accuracy of the data from potential and current aviation workers?

Ms. FITZMAURICE. Thank you. So, you know, we continuously look at this. We, again, we concur with the recommendations that the OIG has made in this area. Going back to 2012, we have been making improvements, putting in system logic so that it will reject information that may be erroneous or inaccurate.



We have also added automation to allow them to upload identity documents so we have that information to be able to review. But looking forward, I think there are continued opportunities. One of the things that we are looking at is further automation in this process.

So the way the information comes from the airport operators through channelers to us is through both automated and some manual processes. We are looking to move to a fully automated process that will reduce the opportunity for erroneous data to be submitted.

Mr. PAYNE. Thank you. I yield back, Mr. Chairman.

Mr. KATKO. Thank you, Mr. Payne. The Chair now recognizes Mr. Ratcliffe from Texas for questioning.

Mr. RATCLIFFE. I thank Chairman Katko and Ranking Member Rice for holding yet another hearing on this matter. I have to say, though, that it feels a little bit like the movie Groundhog Day, where the same things keep happening over and over again.

Inspector General Roth, you are back here again, as you were previously. We have had several hearings on this matter before this subcommittee on security breaches caused by improper screening. Most recently in April, I think, we had then TSA Administrator Carraway talking about the steps that had been taken to make airport and airline employee screening more secure.

But earlier this month, we had the report about officials being able to get banned items through security checkpoints 95 percent of the time. Now, Inspector General, we have got your report revealing that the TSA failed to identify these 73 active workers with links to terrorism, citing a lack of effective controls in your report. I note in your report, you conclude with this statement, "With our recent report, we add another security vulnerability that TSA must now address." I agree with you. TSA does need to address these issues.

As Chairman McCaul noted, it has now been almost 14 years since 9/11. Unfortunately, some of what I see in your report calls to mind the troubling pre-9/11 trend that we had. I know that you are a former Department of Justice official, former assistant United States attorney, I should say. As you know, we had a problem before 9/11 where intelligence and law enforcement were not sharing information and connecting the dots. But we had an excuse back then, the law didn't allow it. So we changed the law to allow the sharing of that information.

So I want to ask you about your report because you say that TSA didn't identify these 73 individuals with links to terrorism because TSA isn't cleared to receive all terrorism categories under the current interagency guidance. Did I restate that accurately?

Mr. ROTH. Yes, sir.

Mr. RATCLIFFE. Okay. You talked a little bit about this with Congressman Rogers, but I am not real clear. Is this a situation where we need to change the law?

Mr. ROTH. It may very well be. My suggestion would be to allow TSA to deal with ODNI, the Office of National Intelligence, and determine whether or not they will be able to have access to this information. If not, it may require a change in the law.

I will say that I share your concerns that information sharing is critical, particularly in this area. Even if there is information that is contained within the TIDE database that is unsubstantiated, it is still useful for individuals doing a manual review of somebody who is going to have unfettered access to secure areas in the airport.

What is very troubling, both about this sort of TIDE database as well as criminal history checks, is that TSA is being treated, for all intents and purposes, as if they were a Wal-Mart, that an individual holding a SIDA badge for recurring criminal history checks, stands in line with Wal-Mart to determine whether or not there will be a criminal history check.

Mr. RATCLIFFE. Okay. Let me ask you about that. Because we talked a little bit about that. In your testimony, you talked about the fact that airport operators review the criminal histories for new applicants for these badges to secure areas, secure airport areas, but that TSA and the airports aren't legally authorized to conduct recurrent criminal history vetting. Is that right?

Mr. ROTH. That is correct.

Mr. RATCLIFFE. So, currently, then, how do TSA and the airports know if an employee has committed a crime during their tenure at the airport?

Mr. ROTH. That is the difficulty of it, and that is why TSA is providing this Rap Back Program, a pilot program that they are going to start at the end of this year, to try to attempt to get recurrent vetting. It is a new program that the FBI has started. But as far as the current conditions, that is a vulnerability.

Mr. RATCLIFFE. Okay. But is TSA right now—are they checking—do they have the ability to check against the Marshals Service Wants and Warrants list?

Ms. FITZMAURICE. Yes, we do check against the open Wants and Warrants for the Marshals Service.

Mr. RATCLIFFE. Okay. But that list doesn't include all disqualifying crimes, correct?

Ms. FITZMAURICE. That is correct. What is really critical here is getting access to the Rap Back capability.

Mr. RATCLIFFE. Okay. I see that my time has expired, so I yield back.

Mr. KATKO. Thank you, Mr. Ratcliffe.

I now recognize the gentleman from Massachusetts, Mr. Keating, for 5 minutes of questioning.

Mr. KEATING. Thank you, Mr. Chairman.

Mr. Ratcliffe mentioned this reminded him of the movie Groundhog Day. This also reminds me of the Leonardo DiCaprio movie, Catch Me If You Can, where he dresses up like an airline pilot, just waltzes right in through security. Because these are very real issues.

We had a hearing of the Oversight Committee, which I was Ranking at the time, at Logan Airport several years ago, and one of the major things that came out of that was the fact that there is real jurisdictional problems with airports that we have. We are hearing it again here today, in very severe terms.

I just want to follow up and say, if you have noncompliance by the municipal airport, what can you do about it? I mean, we found

holes in fences, perimeters not being looked at, and they were cited in vulnerability assessments and other things, and nothing was done because there was no enforcement over those municipal airports or whoever runs the airport authority, whoever runs these things.

We are seeing now in testimony this morning that when you are reviewing some of the employment vetting that is there, that you are doing only 1 percent of it. But you are finding mistakes that they don't do and they didn't come forward with it. Yet, how is that followed up? How are they penalized for that? What are they threatened with for that?

It seems like we have a basic jurisdictional issue aside from information sharing here, where you have Federal agencies that aren't helping each other or giving each other information that they should be giving each other. We are going to change the law to make sure that is the case. Yet, what are you doing with the municipalities?

Now, Ms. Fitzmaurice, there was an effort on the part of TSA to take the exit lanes in that inner security area and move the authority away from TSA employees and give it to the local—give the responsibility to the local municipal employees. Given what we have discussed this morning, is it fair to say that is sufficiently dead? Are you going to stop pushing that effort to get rid of TSA employees and replace them with municipal airport employees, or authority of the airport, you know, their employees?

Are you aware of what that effort has been in the last couple of years trying to shift that responsibility?

Ms. FITZMAURICE. I want to make sure that I am responsive and I understand your question.

You are asking whether we would take back the responsibility of the airport worker?

Mr. KEATING. No. No. You have been asking the airports over the last couple of years to shift the responsibility, take the responsibility with—they are putting their employees now in that exit lane out of the airports in which many airports is right next to where people are coming in. That has been delayed, I think in part, because Members of the committee expressing concerns.

Is it fair to say, given what we are hearing this morning, that that is not going to be pursued anymore?

Ms. FITZMAURICE. You know, I apologize. I don't have an answer for you on that. I will have to get back to you.

Mr. KEATING. Also, when we are looking at the number studies, I want to thank GAO. I mean, on the vulnerability studies on the physical aspects of this, we found that it is less than 3 percent of the airports that are being reviewed. This morning, we found out it is only 1 percent. We also know that the airports aren't doing their job either. It is too many of them. So we have these lapses all the way through. What I would hope, and maybe I can ask Mr. Roth this, do you think there is a need to have more accountability and a better need to enforce the operations of airport authorities and municipal airports as well when they can just look at the recommendations, look at what has been found, and we are not even clear anything's done other than them—they can shrug their shoul-

ders, as they did with perimeter security when we addressed it, just say, well, we don't have the resources for this.

I just don't want to see a situation where we have a strategy and the Federal Government is pointing their finger at municipal airports and the authorities, the authorities are pointing at the Federal Government, our other law enforcements all pointing their fingers. Finger-pointing is dangerous, and it is going to get us nowhere. That is what we have been dealing with in the last few years.

So do you think there is a need to put teeth in what the TSA can do with airports?

Mr. ROTH. You raise a good point. We haven't actually done any work on that, but it is certainly something that we would be willing to consider, which is irrespective of whether TSA follows up and actually finds out, for example, whether the airport officials are doing the criminal history checks that they need to do, when they find noncompliance, what do they do about it? Unfortunately, I don't have the answer to that question, but you raise a very good question and—

Mr. KEATING. The answer when it comes to vulnerability studies, it is a toothless grin, nothing. So let's find out here and put some teeth in what we are trying to do.

I yield back, Mr. Chairman.

Mr. KATKO. Thank you, Mr. Keating.

The Chair now recognizes Mr. Carter from Georgia for 5 minutes of questioning.

Mr. CARTER. Thank you, Mr. Chairman. I appreciate your leadership in this most disturbing situation we find ourselves in.

Mr. Roth, I read your report, and I appreciate it very much, but there were several things in your report that were very disturbing to me, very disturbing.

First of all, it is my understanding that security credentials are being given to individuals regardless of their work or authorization dates. Is that correct?

Mr. ROTH. That is correct. What we had found was, in fact, say you were authorized to work for 18 months, you would get a security badge that would not turn off at the termination of your authority to work.

Mr. CARTER. So what you are telling me is that we might have people, and we may have people, we probably do have people, who are walking around unescorted in our airports and security areas who are here illegally?

Mr. ROTH. Who do not have authorization to work, yes. We identified that as a vulnerability.

Mr. CARTER. You know, certainly—certainly, we have these people's Social Security number, correct?

Mr. ROTH. I am sorry. I missed the question.

Mr. CARTER. Certainly, we have these people's Social Security number? We have that?

Mr. ROTH. We do not, no. That—

Mr. CARTER. Whoa. Whoa. Whoa. We do not. So you are telling me we have got people walking around unescorted in secure areas in our airports, and we don't even have their Social Security number?

Mr. ROTH. That is correct. We did a scrub of the data and found a number of areas in which they don't have either their alien registration number, if that is appropriate, their passport number, if that is appropriate, or their Social Security number.

Mr. CARTER. Holy cow.

Ms. Fitzmaurice, the report in the inspector general's investigation found that we had thousands of incomplete, or inaccurate applications and biographical information.

Can I ask you, Ms. Fitzmaurice—and if you will bear with me, please—can you give me the first initial of your first name?

Ms. FITZMAURICE. S.

Mr. CARTER. S? Now I have got 3 minutes left to ask questions here. Do you think I can guess your first name in that 3 minutes? My point is simply this: We have applications that only have the first initial of the first name?

Ms. FITZMAURICE. That is correct.

Mr. CARTER. Does that scare you?

Ms. FITZMAURICE. So I think we are absolutely looking at and concerned with where we have erroneous and missing information, and we are taking actions. We have already implemented logic in our system to reject these types of—

Mr. CARTER. I appreciate that, Ms. Fitzmaurice. I really do. Look, I am from Georgia. I travel at least once, usually twice, through the busiest airport in the world, through Atlanta Hartsfield-Jackson Airport. To think that we may have people walking around in that airport who we don't even know what their name is. We don't have their Social Security number. I mean, isn't that something—look, I am okay. You know, I am pretty confident I can take care of myself to a certain extent. But my son's coming up later today. I want to make daggone sure he is okay. My younger son's coming up today, my middle son's coming up tomorrow. Isn't this something that should be taken care of immediately? Immediately?

Ms. FITZMAURICE. Yes. We are taking actions immediately to work on continued improvements to improve the data quality for the vetting systems.

Mr. CARTER. I just can't believe that in the world's busiest airport, in Atlanta Hartsfield-Jackson Airport, that we could have people walking around unescorted in secure areas in that airport, who we don't know their Social Security number; we don't know their name, and that is something that we are sitting here talking about? You ought to be on the phone right now. Stop, we have got to figure this out.

I am appalled at this. Mr. Roth, I appreciate the efforts here, and I appreciate all the efforts of all of you, but we need to take care of this immediately.

Mr. Chairman, I yield.

Mr. KATKO. Well, thank you, Mr. Carter. I think the committee shares your frustration, and that is why we had something else scheduled for today here on passenger rail safety and surface transportation safety, but instead we chose to have this hearing.

I want to juxtapose TSA's turtle-like response to seemingly serious problems with what the committee has done. We found out about this less than a week ago. We are having a committee hear-

ing today, and we are marking up a bill to fix this problem right after this hearing.

So the point is, if you have issues, and you need things done, I highly encourage TSA to come to us, because we can give you legislative fixes to things instead of waiting a year to negotiate or hope to get something while the security lapse—securities gaps continue.

Now, I note TSA is working on issues and trying to fix things. Let me tell what you TSA is doing in the mean time.

We had a problem with PreCheck. Our PreCheck bill is going to be introduced next week, or in the next couple of weeks, to deal with expanding, revamping the PreCheck Program and having it being run properly, because they have concluded that it was not. Part of the PreCheck was called Managed Inclusion, we take people out of nonsecure lines and put them into PreCheck because—for keeping to our passengers' flow. That is not right, and that is going to be fixed. Mr. Thompson is introducing a bill regarding that. We have access control and screening issues at airports to employees that are absolutely, positively abysmal. When people are having guns on airplanes, when people are dealing dope out of the Oakland Airport, it is a problem. It can't wait for discussions. We are going to fix that. We are introducing a screening bill next month that is going to fix that.

We also have many other things we are going to be working on. I can tell you going forward, I highly encourage TSA to work with us and not just close ranks and say, we are working, looking into the issue. It is now a year after you found out that your employees were not getting checked against a database, and a year after people started requesting that information happen, and they are still spinning their wheels. That can't happen.

You are entrusted with our Nation's security, our children's security, like Mr. Carter said, and we need to do a better job, we just flat out need to do a better job, and it starts with leadership.

It took us months of begging the President just to appoint a successor for TSA. That is unacceptable in such an important agency. So I can tell you one thing going forward, we are not going to wait for things to happen. We are going to legislate, and we are going to fix these things, because we can't wait for these things to be fixed.

Mr. Roth, I encourage you to keep doing what you are doing. You are doing a superb job at keeping us informed and exposing issues that need to be taken care of. I know it is a lot of work. I can tell you, Ms. Grover, too, what you are doing is critically important to the safety of our country. I applaud both of you and your agencies and your staffs for what you are doing, so keep it up.

Now, with that I want to thank the witnesses for their testimony and the Members for their questions. The Members of the committee may have some additional questions for the witnesses, and we will ask your response to these in writing. The hearing will be held open for 10 days without objection. The committee stands adjourned, but I will note that we are going right to mark up in about 15 minutes after a break, and we are going to have these bills out of committee today, hopefully, and then through the full committee next week and on the floor for a vote. That is how it should be done.

[Whereupon, at 11:21 a.m., the subcommittee was adjourned.]

