S. Hrg. 114–439

OVERSIGHT OF THE TRANSPORTATION SECURITY ADMINISTRATION: FIRST HAND AND GOVERNMENT WATCHDOG ACCOUNTS OF AGENCY CHALLENGES

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

JUNE 9, 2015

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

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE

97–353 PDF WASHINGTON : 2016

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin *Chairman*

JOHN MCCAIN, Arizona
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MICHAEL B. ENZI, Wyoming
KELLY AYOTTE, New Hampshire
JONI ERNST, Iowa
BEN SASSE, Nebraska

THOMAS R. CARPER, Delaware
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana
TAMMY BALDWIN, Wisconsin
HEIDI HEITKAMP, North Dakota
CORY A. BOOKER, New Jersey
GARY C. PETERS, Michigan

KEITH B. ASHDOWN, *Staff Director*
MICHAEL LUEPTOW, *Investigative Counsel*
GABRIELLE A. BATKIN. *Minority Staff Director*
JOHN P. KILVINGTON, *Minority Deputy Staff Director*
BRIAN TURBYFILL, *Minority Senior Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*
LAUREN M. CORCORAN, *Hearing Clerk*

CONTENTS

WITNESSES

TUESDAY, JUNE 9, 2015

ALPHABETICAL LIST OF WITNESSES

APPENDIX

OVERSIGHT OF THE TRANSPORTATION SECURITY ADMINISTRATION: FIRSTHAND AND GOVERNMENT WATCHDOG ACCOUNTS OF AGENCY CHALLENGES

TUESDAY, JUNE 9, 2015

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:34 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Ron Johnson, Chairman of the Committee, presiding.

Present: Senators Johnson, Lankford, Ayotte, Ernst, Sasse, Carper, McCaskill, Baldwin, Booker, and Peters.

OPENING STATEMENT OF CHAIRMAN JOHNSON

Chairman JOHNSON. The Committee will come to order.

I want to first welcome our witnesses. Thank you for your very thoughtful testimony that you have provided in written form, and I am looking forward to your oral testimony and your answers to our questions.

I do want to point out that this hearing is necessary. I think it is unfortunate that some information was leaked prior to our ability to really completely analyze it. We want to make sure, as we are asking questions, as you are answering questions, that we do not reveal classified or sensitive information to give our enemies information to harm us. But the fact of the matter is if we ever are going to solve any problem—and I have said this repeatedly from this chair—we have to recognize and acknowledge reality. We have to describe it.

The purpose of any hearing under my chairmanship is that in the end, following the hearing, every Member on the dais, hopefully every member of the audience, takes the first step in solving any problem, which is admit we have one.

And certainly as I have been reading the briefings, I have been thinking about the struggles with the Transportation Security Administration (TSA) since it was first established, understanding how it has two missions, and they are, by and large, almost completely contradictory.

On the one hand, we are looking for 100 percent security to keep not only just airline but all public transportation 100 percent safe and secure.

On the other hand, we are looking for complete efficiency so that lines do not back up. We are looking for efficient throughput through the system. It is an enormously complex and difficult task, and because of the leaked information—and, Inspector General John Roth, I have to commend you for your independence, for taking a hard look at this, doing the inspections, the investigations that I think are appropriate. We are finding out that that contradictory goal, we are not meeting both of those, not by a long shot.

So certainly with Secretary Johnson, with the Inspector General (IG), with the Acting TSA Administrator now, and the TSA nominee, I have had some pretty serious discussions, and I have asked them to completely analyze the problem, start thinking outside the box. We need to look at more effective solutions, and we have to start prioritizing what we can do that is going to improve security in the most effective way.

An example I will use is, after September 11, 2001 a pretty simple solution has probably provided us the greatest security so that at least airlines cannot be used as the most efficient weapon, most effective weapon, being able to fly into things like the World Trade Center, and that was just locking the doors and securing the cockpit door. But we found out with Germanwings that is not a complete and total solution either. It creates some unintended consequences.

So, again, the point I am making is this is an enormously complex and difficult issue. We need to approach the solution soberly and honestly and lay the problem out.

I would like to, first of all, ask unanimous consent to have my written opening statement entered in the record.[1]

I would also point out that we had another witness, Mr. Jason Harrington, who is unable to make it due to illness. He was a transportation security officer (TSO) at the Chicago O'Hare International Airport from 2007 to 2013. He submitted written testimony in preparation for this hearing, and so I ask unanimous consent to enter his testimony in the record[2] as well.

But I would like to just read a couple stats that kind of describe the difficult mission of the TSA. TSA is compromised of 46,000 transportation security officers. Twenty percent of the TSA employees are veterans. That is a good thing. I would almost like to see that increased.

TSA screens 2 million passengers each day—nearly 160 million every year. That is an enormous challenge and task. TSA screens 1.1 million checked bags and 3 million carry-on bags for explosives and other dangerous items on a daily basis. TSA used more than 700 advanced imaging technology (AIT) machines at airports nationwide.

TSA is responsible for the security of 25,000 domestic flights per day, 2,500 outbound international flights per day. It also secures 4 million miles of roadways, 140,000 miles of railroad track, 600,000 bridges and tunnels, 350 maritime ports, 2.6 million miles of pipeline.

---

[1] The prepared statement of Chairman Johnson appears in the Appendix on page 37.
[2] The prepared statement of Mr. Harrington appears in the Appendix on page 41.

Again, it is an enormous challenge, so we need to recognize that reality and, again, take a look at this problem as one that is a significant challenge and talk about it as honestly as possible if we are going to really find solutions.

With that, I will turn it over to our Ranking Member, Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thanks, Mr. Chairman. Thanks for bringing us all together today. Our thanks to our witnesses. Good to see you all. And thank you for your attendance, your preparation, and your willingness to respond to our questions.

Few Federal agencies interact with the American people more on a daily basis than does TSA. The men and women who work there have, as the Chairman has said, a very difficult but extremely important job.

Last month, I spoke on the Senate floor about two women who have dedicated their lives to keeping our aviation system and its users secure by working for TSA. In fact, one of these two women was shot in the line of duty and showed up for work the very next day. Every day, these women and their colleagues, thousands of them around the country, work in a very challenging environment to keep our aviation system safe and those of us who use it safe and secure. We do not do enough to acknowledge that and to thank them when they do their jobs well, which is almost all the time.

While I believe it is important for us to recognize exemplary performance when it is done at TSA or throughout other parts of the Department of Homeland Security (DHS) more often than we do, this Committee also has an obligation to exercise our oversight responsibilities when performance falls well short of that standard.

Thanks to our witnesses before us today, we have been alerted to a number of instances where performance by TSA and its employees appears to have been disappointing and even troubling. Just yesterday, for example, we learned from the DHS Inspector General that 73 individuals with possible links to terrorism have been granted credentials to access secure areas of airports across our Nation.

And last week, of course, we learned about significant vulnerabilities at passenger screening checkpoints uncovered by the Inspector General. The reported failure rates for detecting prohibited items at checkpoints are more than troubling. They are unacceptable. And I look forward to reviewing the Department of Homeland Security Inspector General's full report and recommendations later this summer. That said, I am encouraged by the swift action taken by the Secretary of Homeland Security to address the Inspector General's findings.

Since 2011, the Transportation Security Administration has transitioned from a one-size-fits-all screening philosophy to one that is more risk-based. That approach is designed to allow TSA to deploy its limited resources to the areas where we face the greatest threat.

However, as the Inspector General and the General Accountability Office (GAO) have identified, such a swift transition may have created vulnerabilities in the system. Given recent reports, it

is more important than ever for the Transportation Security Administration to have a permanent, Senate-confirmed leader in place. I thank the Chairman and his staff for working so quickly and cooperatively with my staff so that we can move the nomination of Vice Admiral Peter V. Neffenger, which we will examine in a hearing tomorrow.

With that, we look forward to the testimony, and we thank the witnesses for appearing here today. I am grateful that the current front-line employees have joined us today to discuss their perspectives on how to improve TSA.

I will close with one last personal thought. My father used to drive my sister and me crazy when we were kids growing up by saying some of the same things over and over and over again. And one of these things he said over and over again is that if the job is worth doing, it is worth doing well. He said that hundreds of times, maybe thousands of times. And out of that I took this lesson: We should be focused on perfection. We will never get there, but that should be our goal. And if it is not perfect, we need to make it better.

Clearly, there are some things going on at TSA that fall well short of perfection. Our job is to help you get closer, help them help TSA to get closer to that goal to better protect the people who use the airlines, including all of us.

Thank you so much.

Chairman JOHNSON. Thank you, Senator Carper. I would only add that in our quest for perfection, the way you achieve it is through continuous improvement. I think that is the right kind of attitude here.

It is the tradition of this Committee to swear in witnesses, so if you will all stand and raise your right hand. Do you swear that the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. ROTH. I do.

Ms. GROVER. I do.

Mr. MACLEAN. I do.

Ms. ROERING. I do.

Chairman JOHNSON. Thank you. Please be seated.

Our first witness is John Roth. Mr. Roth is the Inspector General for the Department of Homeland Security. Prior to serving as DHS's Inspector General, Mr. Roth was Director of the Office of Criminal Investigations at the Food and Drug Administration (FDA) and also had a decorated career as a Federal prosecutor with the Department of Justice (DOJ).

Inspector General Roth.

TESTIMONY OF HONORABLE JOHN ROTH,[1] INSPECTOR GENERAL, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. ROTH. Chairman Johnson, Ranking Member Carper, and Members of the Committee, thank you for inviting me here to testify today to discuss our work examining TSA's programs and operations.

[1] The prepared statement of Hon. Roth appears in the Appendix on page 45.

Before discussing TSA's challenges, I would like to acknowledge the TSA whistleblowers that I join on this panel today. We are grateful when TSA employees—as well as employees from other parts of the Department of Homeland Security—are willing to step forward to identify problems within the agency. Whistleblower disclosures have saved lives as well as taxpayer dollars, and whistleblowers play a crucial role in keeping our Department efficient and accountable.

We review over 16,000 complaints per year, more than 300 per week, to better understand and respond to potential waste, fraud, and abuse in the Department's programs and operations.

With regard to TSA, we face a classic asymmetric threat in attempting to secure our transportation systems: TSA cannot afford to miss a single, genuine threat without potentially catastrophic consequences, yet a terrorist only needs to get it right once. TSA's thousands of transportation security officers conduct tedious tasks that require constant vigilance. Complacency can be a huge detriment to TSA's ability to carry out its mission. Ensuring consistency across DHS's largest workforce would challenge even the best of organizations.

Unfortunately, although nearly 14 years have passed since TSA's inception, we remain deeply concerned about its ability to execute its important mission. Since 2004, we have published more than 115 audit and inspection reports about TSA's programs and operations. We have issued hundreds of recommendations to attempt to improve TSA's efficiency and effectiveness.

We have conducted a series of covert penetration tests—essentially testing TSA's ability to stop us from bringing in simulated explosives and weapons through checkpoints, as well as testing whether we could enter secured areas through other means. We identified vulnerabilities caused by human and technology-based failures.

I am aware of the media reports regarding our most recent testing. Although the details of those tests are classified, and I will not be able to speak to the specifics of them in the hearing today, I welcome the opportunity to brief Members of this Committee and their staff regarding our findings in an appropriate and closed setting.

We have also audited and reported on TSA's acquisitions. Our audit results show that TSA faces significant challenges in contracting for goods and services. Despite spending billions on aviation security technology, our testing of certain systems has revealed no resulting improvement.

We have examined TSA's approach to risk-based screening. While we applaud the concept of a risk-based approach in transportation security, our audits and inspections have uncovered significant vulnerabilities, and we have deep concerns regarding the manner in which TSA manages this risk. This includes TSA's use of managed inclusion, its risk assessment rule in granting expedited screening to those who are not part of PreCheck, and the administration of the PreCheck program itself.

We have also examined the performance of TSA's workforce, which is largely a function of who is hired and how they are trained and managed. Our audits have repeatedly found that

human error—often a simple failure to follow protocol every time—poses significant vulnerabilities.

We have also looked at how TSA plans for, buys, deploys, and maintains its equipment and have found challenges at every step in the process. These weaknesses have a real and negative impact on transportation security as well.

TSA has taken some steps to implement our recommendations and address security vulnerabilities. Nevertheless, some problems appear to persist. While TSA cannot control all risks to transportation security, many issues are well within its control. Sound planning and strategies for efficiently acquiring, using, and maintaining screening equipment, for example, would go a long way toward improving overall operations. TSA needs to have a better understanding of the limitations of its technology and develop strategies to counter those limitations. Better training and better management of TSOs would help mitigate the effects of human error that, although never eliminated, could be reduced.

Taken together, TSA's focus on management practices and oversight of its technical assets and workforce would help enhance security as well as customer service for air passengers.

Mr. Chairman, this concludes my prepared statement. I am happy to take any questions you or other Members of the Committee may have. Thank you.

Chairman JOHNSON. Thank you, Mr. Inspector General.

Our next witness is Rebecca Roering. Ms. Roering is the Assistant Federal Security Director for Inspections at the Minneapolis-St. Paul International Airport. During her 25 years of government service, Ms. Roering has also served the Federal Aviation Administration (FAA) as a Federal Air Marshal (FAM) and Civil Aviation Security Inspector. Ms. Roering.

TESTIMONY OF REBECCA ROERING,[1] ASSISTANT FEDERAL SECURITY DIRECTOR—INSPECTIONS, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. ROERING. Chairman Johnson, Ranking Member Carper, and Members of the Committee, thank you for inviting me here today to discuss important security concerns related to the TSA and security at our Nation's airports.

The mission of TSA is to ensure the freedom of movement for people and commerce, which is undeniably a difficult challenge. It is also the mission of TSA to protect the traveling public against terrorist attacks. The ability of TSA to execute its mission has been called into question by many oversight groups.

My testimony today will focus on a number of the security concerns and agency policies that result in vulnerabilities and morale issues across our workforce.

Over recent years, TSA has hired into leadership positions a number of former airline executives and others who place more emphasis on customer service and passenger wait times than on security and detection rates. Any wait time that is deemed by the agency as excessive requires immediate reporting, a thorough analysis,

[1] The prepared statement of Ms. Roering appears in the Appendix on page 59.

and corrective action. Conversely, the local monthly testing of our officers to determine their ability to detect weapons and explosives is not associated with any performance metric. When this testing results in a failure to detect the item, there is basic remedial training required before the officer may return to duty. A TSA officer may never be subjected to a covert test based on the current volume of assigned tests each month, limited resources to conduct the tests, and the sheer volume of our officers. This lack of realistic testing on a regular basis leads to complacency in our workforce.

It is not until recently, actually within the last few weeks, that detection rates of improvised explosive devices (IEDs) has become a topic of discussion at TSA. This is the direct result of covert testing at numerous airports identifying detection rates that caused great concern. Leadership recognized that poor detection rates are, in part, related to the poor morale that exists across our workforce.

The 2014 Federal Employee Viewpoint Survey resulted in the DHS receiving among the lowest ratings of any Federal Government agency, and TSA receiving more than their fair share of low marks. The survey demonstrated that while our frontline employees feel strongly that the work they do is important, they are not valued by our leadership. The job of a TSA officer is a challenging one, with a great deal of pressure and scrutiny. A culture of fear and distrust has been created in the agency, also impacting the morale and performance of our employees. This is clearly documented in the results of the survey.

Equally as troubling are the security gaps associated with the TSA PreCheck program. While a risk-based approach to security screening is essential, TSA has expanded PreCheck to large populations of passengers who have not enrolled in or paid for the program. In the fall of 2013, I expressed my concerns with the expansion of PreCheck to my leadership as well as the TSA Office of Inspections (OOI). I later reported the concerns to the Office of Special Counsel (OSC) for investigation. My allegations were substantiated by the DHS Inspector General in a report titled "Security Enhancements Needed to the TSA PreCheck Initiative."

TSA is handing out PreCheck status like Halloween candy in an effort to expedite passengers as quickly as possible, despite self-admitted security gaps that are being created by the process. The TSA PreCheck enrollment program did not meet the expectations in terms of volume; therefore, PreCheck rules keep expanding as a matter of efficiency even though the agency is well aware of the associated risks.

As documented in recent reports, the insider threat continues to present a security concern at our Nation's airports. Although some form of screening is conducted on cargo that is transported on passenger aircraft, catering supplies, checked baggage, and, of course, passengers, there are other airport employees who have access to sterile areas of the airport who are subjected to only criminal history record checks and security threat assessments. This group has unimpeded access to aircraft, and it was discovered that some of these security identification display area (SIDA) badged employees who had worked at the Minneapolis-St.Paul (MSP) Airport later traveled to Syria to fight for the Islamic State of Iraq and the Le-

vant (ISIL). TSA has increased the use of Playbook teams recently with a focus on insider threat.

At many locations, and in my experience, the Federal Security Director (FSD) is reluctant to initiate enforcement action against the airport or air carriers. A conflict of interest exists when the FSD relies upon the airport and air carrier to provide certain services and, on the other hand, has overall responsibility for the execution of the regulatory program.

Additionally, transportation security inspectors are being used by FSDs to perform a wide range of duties not related to their core functions. Such duties include moving bins at the checkpoints and conducting audits of Universal Enrollment Facilities to determine such items as whether or not there is hand soap in the restrooms or if the staff is friendly. These audits should be done by a contracting officer rather than regulatory inspectors. DHS should reconsider the reporting structure for our inspectors to eliminate any potential conflicts, misuse of their time, and pressure to avoid enforcement actions.

TSA uses prohibited personnel practices to pressure employees to resign when management wants them removed from the agency. When allegations of misconduct occur by employees in certain positions, the FSD must refer the allegations to the TSA Office of Inspection. If the Office of Inspection does investigate, they send criminal investigators to conduct investigations of even minor administrative matters. It is a waste of taxpayer dollars to use criminal investigators to conduct routine administrative investigations and also destroys the morale and trust of our workforce.

In conclusion, the culture that exists at TSA is one of fear and distrust. While TSA cannot control all the risks associated with aviation security, leadership of the agency is certainly in a position to impact change. Better training and management of the workforce would result in an improvement to morale as well as detection rates. If a TSA employee feels valued and respected, the metrics will reflect this in a positive way. TSA should eliminate security gaps created by risk assessment rules in PreCheck, and DHS should reconsider the reporting structure for Inspectors to avoid any conflicts.

Mr. Chairman, this concludes my prepared statement. I welcome any questions from you or any Members of the Committee. Thank you.

Chairman JOHNSON. Thank you, Ms. Roering.

Our next witness is Robert MacLean. Mr. MacLean is a Federal Air Marshal who blew the whistle about potential safety concerns regarding a TSA plan to alter mission schedules. Mr. MacLean was fired by TSA for disclosing this information, but he was eventually reinstated after successfully appealing his improper termination before the U.S. Supreme Court. He is currently a Federal Air Marshal based out of Los Angeles Field Office. Mr. MacLean.

TESTIMONY OF ROBERT J. MACLEAN,[1] FEDERAL AIR MARSHAL, OFFICE OF LAW ENFORCEMENT, FEDERAL AIR MARSHAL SERVICE, TRANSPORTATION ATTORNEY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. MACLEAN. Thank you, Chairman Johnson, Ranking Member Carper, and other Members of the Committee. It is a great honor to be here as an active-duty TSA Federal Air Marshal.

Due to my 12-year case that finished before the Supreme Court 4 years ago and my role as a national whistleblower liaison for the Federal Law Enforcement Officers Association (FLEOA), which is not a union, dozens of TSA Federal Air Marshals come to me with their concerns about aviation security threats. This is a huge responsibility, being a voice for those who are tasked with stopping terrorism.

The public wants to continue enjoying the great privilege and miracle of flying on jetliners. They are tired of the complaints and want their tax money spent wisely on realistic measures. The 9/11 attacks should have proved how volatile it is inside a crowded, pressurized thin tube traveling 500 miles per hour 40,000 feet up in the sky.

Air Marshals' most common concern: improved explosive devices, bombs. If a terrorist group puts thought into it, it is relatively easy to sneak small bombs into jets in order to blow up at high altitude. Bombs just will not pass through checkpoints, but purposely or not wittingly by airport workers or delivery drivers bringing in daily mega tons of items consumed by passengers in the boarding areas. That cargo includes food, drink, condiments, cooking oil, cleaning products, and then all of the packaging that goes with it. Then you have all of the dense stacks of newspapers, magazines, and books. This mountain is nowhere near getting the screening that passengers are getting at the checkpoints. A bomb smuggler will hide a needle in a hay wagon before sneaking a steak past a pack of wolves.

One remedy: take more TSOs off checkpoints and get exhausted Air Marshals out of airline chairs and deploy them deep inside the bowels of the train stations and airports to do traditional foot patrol, such as the uniformed Visible Intermodal Prevention and Response Teams (VIPR) and the undercover Red Teams.

When I flew missions, I desperately tried to find that terrorist. But instead I disrupted three illegal alien-smuggling operations purely because of my experience learning the mundane routines of the traveling public, building rapport with the airport workers and local authorities, knowing the area real well, and just simply reading faces.

TSA PreCheck, with the improvements Ms. Roering obviously pointed out, should be greatly expanded, and it should be free of charge. More people in PreCheck frees up resources to focus on attackers. I would like to see TSOs roaming airports with mobile PreCheck application kits and soliciting passengers during their delays.

We need to have more faith in human intelligence gathering and the intuition of bold officers. But in order to get more Air Marshals

[1] The prepared statement of Mr. MacLean appears in the Appendix on page 68.

on the ground, you need to completely secure the flight deck or the cockpit where the pilots are in control of the jet. Every flight deck should have a modified shotgun with an emergency lock switch. Shotgun pellets are ideal since the primary concern is to stop an attacker trying to force the door open. In a highly unlikely miss, shotgun pellets will not harm passengers or the aircraft. The group of pilots who use their own funds to travel to Artesia, New Mexico, spending a week being trained and issued a TSA .40-caliber semi-automatic pistol can miss and kill an innocent passenger in the very back of the cabin with a jacketed bullet. Once again, this is highly unlikely, but it is possible.

Armed pilots are not allowed to carry their pistols on international flights due to very restrictive handgun laws in foreign countries. But a shotgun modified to stop one or two hijackers trying to break into the cockpit from 1 foot away would be inane for a host country to deny and risk another 9/11-style attack. It is an extreme hazard whenever a pilot opens the flight deck door to use the lavatory or to get food and drink. An amped-up attacker can dive inside and destroy the jet.

There is a cheap and perfect solution to this: secondary barriers. Ten horizontal cables attached to a vertical pole, a flight attendant can simply stretch across the front of the forward galley and lock in place. This barrier buys the flight crew plenty of time to quickly get the pilot back into the flight deck and lock the door.

In order to control unruly passengers who could be suicidal attackers setting up a ruse for the law enforcement officers on board, every cabin should be equipped with restraint systems and nonlethal tools to restrain unruly passengers or stop murderous attackers. Flight crews and law enforcement officers need the legal authority to deputize and indemnify vetted, able-bodied passengers to protect themselves and the jet from destruction. We could do this process during our PreCheck. There is no reason why an athlete or a military member cannot walk deep into the cabin to restrain somebody. During PreCheck enrollment, we can ask passengers to volunteer to be these Deputy Air Marshals during critical events and qualify them at training centers.

Passengers may do nothing because of the potential civil liability and because they are expecting Air Marshals to respond. An Air Marshal taken away from protecting the flight deck endangers the entire jet. The pilots may not be able to safely land a jet for hours over an ocean while attackers are going on a murder spree.

In the case of absolute chaos in the cabin, the pilots need the ability to disorient attackers by shutting off all lighting or flashing blinding strobe lights or high-pitched sound alarms. And when that does not stop the mayhem, pilots can actually don oxygen masks and depressurize the cabin, knocking out the attackers due to the rapid breathing and heart rate. Do all of this and give the flight attendants and regular passengers the right to save their lives or the lives of others on the ground.

You can assign Air Marshals in airports to find terrorists and bombs before they go up in the sky. Hiring thousands of flying Air Marshals after 9/11 was a natural reaction, but it should have only been a temporary detail and not a career. Not very many young and ambitious people yearn for a career mostly in an airline seat.

When I was recruited, the experienced Air Marshals told me half the job would be flying, and the rest would be time to recover, train, and investigate. They stress that no one can sustain 5 years of flying 4 to 5 days a week. Fourteen years later, Air Marshals tell me there are still not ground opportunities. We should train Federal and local law enforcement officers to quickly deploy as reserve Air Marshals in order to respond to specific threats.

Finally, all Federal employees are reluctant to report money wasted and dangerous security lapses because they do not want to gamble with their careers before the Merit Systems Protection Board (MSPB), the tiny underfunded agency that rules on whistleblower reprisal claims. For instance, FAA Aircraft Cabin Safety Inspector Kimberly Farrington blew the whistle on FAA 12 years ago. Her case was remanded several times to administrative judge, and in the last remand, she had a hearing 18 months ago and still the judge has not made a decision.

If I had a jury, I would have won 6 years ago. Federal employees are the only workers in the United States who do not have access to jury trials. A restaurant cook reporting spoiled food being served has more due process than an Air Marshal reporting security lapses that can kill hundreds of passengers and cripple the aviation industry.

The list goes on of about what Air Marshals echo to me, so I have availed myself all week to meet with Members of Congress and my fellow TSA force. Many may think my proposals here are risky or even crazy, but I am limited in my opening statement to go into detail about how the benefits can greatly outweigh the risks. Other Air Marshals and I are just doing our best to think like a suicidal attacker. I hope we do not need another 9/11 to prove we were accurate.

I am excited to serve with the new leader of the TSA, Admiral Peter Neffenger. I really hope that he is soon confirmed. I look forward to answering your questions. Thank you. I apologize for going over time.

Chairman JOHNSON. I appreciate your testimony and your willingness to blow the whistle, the courage to blow the whistle.

Our next witness is Jennifer Grover. Ms. Grover is the Director of Transportation Security and Coast Guard Issues for the Government Accountability Office. Ms. Grover's work with the GAO includes assessing the vulnerabilities throughout the TSA's screening process. Ms. Grover.

TESTIMONY OF JENNIFER GROVER,[1] DIRECTOR, TRANSPORTATION SECURITY AND COAST GUARD ISSUES, HOMELAND SECURITY AND JUSTICE TEAM, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. GROVER. Thank you. Good morning, Chairman Johnson, Ranking Member Carper, other Members, and staff. Last week, renewed concerns arose about TSA's screening systems and whether they are sufficient to identify prohibited items.

TSA has developed a layered security approach that is sound in principle, and GAO supports TSA's move toward risk-based screen-

[1] The prepared statement of Ms. Grover appears in the Appendix on page 93.

ing. But to fully deliver the promised security protections under both traditional and expedited screening, TSA must do two things: first, take more rigorous steps to ensure that each layer of security works as intended; and, second, put systems in place to continuously monitor their effectiveness.

Over many years, GAO has reported weaknesses in TSA's oversight of its screening systems, raising questions about whether TSA is falling short in its ability to ensure aviation security. TSA has taken steps to improve oversight of these systems, but additional actions are needed.

Today we will focus on four areas: first, the Secure Flight Program, which matches passenger information against Federal Government watchlists to identify those who should not fly or should receive enhanced screening; second, the AIT systems, which are the full-body scanners used to screen passengers for prohibited items at the checkpoint; third, the managed inclusion screening process, which TSA uses to provide expedited screening to passengers not previously identified as low risk; and, fourth, criminal history checks done to vet airport workers.

First of all, regarding Secure Flight, we found in September 2014 that TSA did not have timely or reliable information about the extent or causes of system matching errors, which occur when Secure Flight fails to identify passengers who were actual matches to the watchlist. In response to our recommendations, TSA has developed a mechanism to keep track of known matching errors and is considering methods to evaluate overall Secure Flight matching accuracy rates on an ongoing basis.

Second, regarding the AIT body scanners, we found in March 2014 that TSA did not include information about screener performance when they were evaluating AIT effectiveness; rather, TSA's assessment was limited to the accuracy of the AIT systems in the laboratory. However, after an AIT machine identifies a potential threat, a screening officer has to do a targeted patdown to resolve the alarm. Thus, the consistency with which the screeners conduct the patdowns properly and identify all threat items is key to ensuring the effectiveness of the AIT systems in the airport operating environment. Consequently, we recommended that TSA assess AIT effectiveness as a function of both the technology and the screening officers who operate it. TSA concurred with the recommendation and recently sent updated information about their efforts to address it, which are under review within GAO.

Third, in December 2014, we found that TSA had not tested the security effectiveness of the managed inclusion process as it functions as a whole. As part of managed inclusion, TSA uses multiple layers of security, such as explosives detection devices and canines, to mitigate the inherent risk that is associated with screening randomly selected passengers in a system that was designed for low-risk passengers. However, if these security layers are not working as intended, then TSA may not be sufficiently screening passengers. TSA has tested the individual layers of security used in managed inclusion and reported them to be effective, but GAO has raised concerns about the effectiveness of some of those layers, such as the behavior detection officers (BDO). TSA is planning to complete testing of the managed inclusion system by mid-2016.

Finally, regarding TSA's involvement in airport worker vetting, we found in December 2011 that TSA and airports were conducting background checks based on limited criminal history information. Specifically, TSA's level of access to the Federal Bureau of Investigations (FBI) criminal history records was excluding many State records. In response to our recommendation, TSA and the FBI confirmed that there was a risk of incomplete information, and the FBI has since reported expanding the criminal history records it provides to TSA for these security threat assessments.

In conclusion, TSA has made progress improving its screening oversight, such as taking steps to assess the vulnerabilities in the Secure Flight Program and by working with the FBI to obtain access to more complete criminal background information. Yet more work remains to ensure that Secure Flight, AIT, and managed inclusion are working as TSA intends.

Chairman Johnson, Ranking Member Carper, this concludes my statement, and I look forward to your questions.

Chairman JOHNSON. Thank you, Ms. Grover.

Inspector General Roth, I want to start with you, and I want to be careful in the way I ask the question, but can you speak to the level of preparation, the level of sophistication of the people on the Red Team in trying to assess the effectiveness of the system?

Mr. ROTH. That is going to be a very difficult question to answer in this environment. I will say that the testers we used are auditors. These are members of the OIG workforce. They do not have any specialized background or training in this kind of work. But, again, to go into more detail about this I think would be problematic.

Chairman JOHNSON. OK. There are a bunch of accountants, which, I am an accountant as well, so——

Mr. ROTH. No insult to accountants. [Laughter.]

Chairman JOHNSON. Can you speak to differences between airports? Did we see some airports perform a whole lot better than others so we could maybe see what works and what does not work?

Mr. ROTH. Again, I cannot get into the specifics of the actual results of the testing, and you should know that we have done field work in this area, but we have not written a report yet.

Chairman JOHNSON. OK.

Mr. ROTH. The chronology is we do field work, and then we analyze the results, sort of do the kinds of comparisons that you are talking about, and then report them out.

Chairman JOHNSON. OK.

Mr. ROTH. I will say, though, that the results were consistent across airports.

Chairman JOHNSON. OK. I understand, so I will not go any further than that.

I would like to talk about just the number of standard operating procedures (SOP), the number of protocols. Maybe Ms. Roering or whoever else wants to speak to that, how many are there? I mean, I will see a briefing. I have seen all the acronyms, and the point I am trying to make is how overwhelming these detailed standard operating procedures are for individual TSOs.

Ms. ROERING. Thank you for the question. Yes, sir, our number of standard operating procedures, offhand I do not know the spe-

cific number, but I can say there is a checkpoint SOP, a checked baggage SOP, an SOP for the ticket documenter/checker position, known crew member SOP, a BDO SOP, a passenger screening canine SOP, and those are just the ones I can think of off the top of my head.

Chairman JOHNSON. There are a lot more. How detailed are all those SOPs?

Ms. ROERING. They are very detailed.

Chairman JOHNSON. So, again, we are just humans, and it is kind of hard to have at your fingertips and the training involved of having somebody be able to follow every one of those SOPs with, again, the volume, the throughput that we are trying to achieve, is a real problem, isn't it?

Ms. ROERING. There are a number of very specific procedures in the SOP. During the training process, the SOPs are separated out so when you are being trained in that function, you would be referring to the SOP that applies.

Some of the SOPs do not apply to all our officers across the workforce. For example, the BDO SOP would not need to be—a normal TSO would not need to know those SOPs as well as the managed inclusion and passenger screening canine SOP. So while there are a number of them, you do not have to be proficient in every single one of the SOPs.

Chairman JOHNSON. In the first round of questioning, I do want to get into the PreCheck Program and my concern that what I think is a really good idea—and I think most people would agree it is a really good idea, but only if completely followed and only if we do complete background checks. So whoever is best able to answer the question in terms of how many people have been cleared for PreCheck—I have information here that it is about 100,000, but I am not sure that is accurate. And of the number that have been cleared, how many actually went through a thorough vetting that we would expect versus under pressure to, again, accomplish the throughput objective, how many have been approved in a very watered-down process? Ms. Grover, you seem to be ready to answer the question.

Ms. GROVER. Yes, sir. I believe that there are about a million people now who have applied for PreCheck, but there are about 7.2 million people who have a Known Traveler Number (KTN) who would routinely get PreCheck on their boarding pass because of their affiliation with certain groups, such as people who are in the Customs and Border Protection (CBP) Trusted Traveler Programs or DOD active-duty military. And then, of course, in addition to that, as was discussed earlier, there are people who can get PreCheck on a one-time basis through TSA's automated risk assessments or at the airport through random selection for managed inclusion.

Chairman JOHNSON. OK. Talk to me a little bit about automated risk assessment.

Ms. GROVER. Yes, sir, automated risk assessment. So the first thing that TSA does is they check to see if a passenger is on one of the terrorist watchlists. If they are not, then TSA checks to see if the person is already a known traveler, so signed up with PreCheck and has a Known Traveler Number.

If not, then all of the rest of the passengers are screened against a set of risk rules that TSA has designed based on intelligence and based on certain characteristics of the traveling passenger, including information about that specific flight that they are looking at. Then the individual can receive PreCheck on their boarding pass on a one-time basis.

Chairman JOHNSON. Would anybody else like to comment on, again, kind of the watering down of the vetting process? Mr. Roth.

Mr. ROTH. And just so you understand, TSA has increased dramatically the use of PreCheck over the last several years. It has gone from really a test kind of a case to a situation where between 40 and 50 percent of all the traveling public gets an expedited screening, whether it is through managed inclusion, whether it is part of a Government Trusted Traveler Program, or whether it is through, as Ms. Grover talked about, these risk rules that apply——

Chairman JOHNSON. So, again, as PreCheck was originally conceived with a full vetting process, how many people received the full vetting process to now 40 to 50 percent of the traveling public qualifying for PreCheck?

Mr. ROTH. TSA recently celebrated a million people who have applied for PreCheck through that vetting program. As Ms. Grover says, there are other Trusted Traveler Programs. For example, CBP has a Trusted Traveler Program that is very similar to PreCheck, actually more extensive than PreCheck. So those folks get grandfathered in. Obviously, Members of Congress and other trusted populations get grandfathered in. But, again, you are talking about 1.8 million people per day traveling, so you are talking about a significant portion of the flying public that is truly unknown to TSA, and yet goes through expedited screening.

Chairman JOHNSON. And waving them through. OK. Well, I am out of time. Senator Carper.

Senator CARPER. Again, thanks so much for joining us today and for your testimony and for your work.

Before we talk about some things that TSA needs to do better, let us talk about—each of you just maybe give us one thing that they are doing well. Give us just one thing that they are doing well, and, John, would you just lead us off there, please?

Mr. ROTH. I mean, certainly, and that is the hazard that I have in this occupation. I only focus on the negative as opposed to the positive.

Senator CARPER. We never do that in our jobs. [Laughter.]

Mr. ROTH. Certainly, the two people sitting to my left are people with courage to sort of see something that has gone wrong and try to fix it, and I suspect within the TSA population there are people every day, thousands of people who get up and put on that uniform and go to work and try to do their best every single day. Again, when you only focus on the negatives, you forget about the overwhelming majority of that population that really wants to do the right thing and cares about their job.

Senator CARPER. Let me just interrupt you for a second, and I want the others to speak. I fly a fair amount, not as much as some of my colleagues. Most of my next flights are on trains. But I have taken over the years to—when someone from TSA is actually doing

a good job, they are polite, they are courteous, they are thorough, I thank them for what they do. They have no idea who I am. They think I am Ron Johnson. [Laughter.]

Chairman JOHNSON. Is that a good thing or a bad thing?

Senator CARPER. Day to day, it is probably mixed.

But that is something we might want to think of. One of the things that makes people like their job is they know what they are doing is important and they feel like they are making progress. We just had an interesting study about a month or two ago that said—it was very senior-level positions in the Federal Government, why people are leaving, and it is because—one of the things is that, as hard as they work, they never get thanked. And it is a little thing, but it is something that we might want to keep in mind.

On the other hand, when somebody is out of order, doing things inappropriate, I will tell them and tell them who I am.

But, anyway, let me jump to Rebecca. Ms. Roering, give us one thing that they are doing well.

Ms. ROERING. I think risk-based security is a good procedure, and as long as there is not risks associated with it—99.999 percent of the traveling public simply wants to get from Point A to Point B safely and securely, and we need to focus on a way to quickly expedite those passengers and focus on that very small percentage of people that actually pose a threat to aviation security. The only way that we can do that is using a risk-based security approach.

Senator CARPER. All right. Thanks.

Mr. MacLean, just very briefly.

Mr. MACLEAN. Once again, I really like the PreCheck Program. It just blows away hay from that haystack so that we can get down to that one needle.

Senator CARPER. That is a good point.

Mr. MACLEAN. And then the other program I really love is the VIPR Teams. I really want officers down deep in those airports establishing relationships with the guy whose job is to mop up hydraulic fluid. He probably is——

Senator CARPER. OK. Hold it right there. I am going to run out of time.

Mr. MACLEAN. Sure.

Senator CARPER. Those are good points. Thank you.

Ms. Grover, at least one good thing.

Ms. GROVER. Yes, sir. I would like to echo what you have previously heard and say that risk-based security at TSA has the opportunity to offer tremendous efficiencies. So I would encourage them to go ahead and continue to work on that.

Senator CARPER. All right. Good.

The most important element of any organization I have ever been a part of or seen is leadership. If you have great leadership, you have a fighting chance to be successful. If you do not, you are probably doomed. And I think we have an—John Pistole was a good leader, had a lot of respect here, certainly by me and I think on a bipartisan basis. The President has seen fit to nominate Admiral Neffenger. I think he is an excellent choice, and we will have a hearing, and we are doing our vetting for him right now.

Again, if Admiral Neffenger were here and you had the opportunity to say this would be a top priority for you, Admiral, what would a top priority be? Ms. Grover, what would you say?

Ms. GROVER. I would go back and echo the remarks that Chairman Johnson made at the beginning and just point out that TSA's primary mission is to ensure aviation security. And another important competing mission is to ensure the free flow of commerce and passengers. Those goals are in tension. And so at this time, when questions have been raised about whether or not the fundamentals are working properly, it is important to have a strong leader in place to be able to guide the organization to figure out how to balance those two elements.

Senator CARPER. Good. Thank you.

Mr. MacLean, one piece of advice for Admiral Neffenger if he is confirmed.

Mr. MACLEAN. More emphasis on protecting the flight deck or the cockpit.

Chairman CARPER. OK. Thank you. Ms. Roering.

Ms. ROERING. I think that the leadership of the agency is one that really focuses on wait times, and we need to focus less on wait times and be more concerned about detection rates and giving our officers the time they need to process the passengers and bags in a manner that they feel that is comfortable the bag does not contain a weapon or a prohibited item.

Senator CARPER. All right. Thank you. General Roth.

Mr. ROTH. I had the good fortune of meeting with the Admiral prior to one of his hearings, and I think the biggest thing that he needs to understand—and I think he does understand this—is an acknowledgment that there is a significant challenge here. I am not sure that that has been embraced TSA-wide. So in order to fix a problem, you have to fully understand it, and I think he is committed to doing that.

Senator CARPER. All right. My last question is similar to my first two: Give us some good advice. Just come back and pick up one point that you mentioned for us, a to-do list for us. GAO gives us its great high-risk list every 2 years. That is our to-do list in terms of ferreting out waste, fraud, and abuse. General Roth, I will ask you to give us one great "to-do" for our list, besides maybe confirming a good leader, but give us one really good one.

Mr. ROTH. Understand the risks that you are attempting to manage. In other words, understand the risks behind the technology, understand the risks behind your management processes and manage against those risks. But if you do not understand those risks, you are not going to be able to manage against it.

Senator CARPER. Thank you. Ms. Roering.

Ms. ROERING. I will take one out of my statement, and that has to do with the fact that we have nobody in the field overseeing the numerous contracts that TSA has engaged in. We have no way to measure if the performance of the contracts is acceptable. Having contracting officer technical representatives (COTR) in the field would let us manage those contracts better so we are not wasting taxpayer dollars.

Senator CARPER. OK. Mr. MacLean, one quick one.

Mr. MACLEAN. I would pass a law that gives flight attendants more training and authority to have passengers save their lives.

Senator CARPER. All right. Thank you. Ms. Grover.

Ms. GROVER. GAO is a data-driven organization, so I would like to see you hold TSA's top leaders accountable by asking for data on the effectiveness of their operations.

Senator CARPER. Good. What you cannot measure you cannot manage. Thank you.

Chairman JOHNSON. Thank you, Senator Carper.

I do have to give a shout out to my TSA TSOs in my gate area C in Milwaukee airport. I travel pretty light, but I did attend a Boy Scout event, and I was rushing to the airport. They gave me this little package I put in my briefcase, and it was a little Boy Scout knife, and they caught it. So, I mean, again, there are, I think, the vast majority of TSO and TSA employees that are trying to, in a very difficult task, stay alert and protect the public. That was my own little experience. I got caught. Senator Ernst.

OPENING STATEMENT OF SENATOR ERNST

Senator ERNST. Thank you, Mr. Chairman, and thank you, Ranking Member Carper, for calling this very timely hearing today, and I do want to thank all of our witnesses with us today. We appreciate your testimony very much.

Senator Carper I think touched on a lot of the questions that I really had. I do believe that there has been an issue with a lack of consistency, and I think it is something that TSA has been suffering for from across the various aspects of the organization and its mission for a while now.

But referenced in all of your testimonies really across the board is varying degrees of lack of certainty and consistency with people, processes, and operations. And these problems, whether it is the morale of the organization, the personnel, or the day-to-day operations, they are just so systemic. So you have mentioned some ideas on where you would like to see leadership go, a couple of suggestions for Congress. But bottom line, do you think it is really more of a management issue for the Admiral? Hopefully he will be confirmed shortly, but are these the issues that the Admiral can influence through his management style? Or is it something that needs to be addressed through legislation? I would like to hear the perspective that you have on that, one or the other or a combination of both. Ms. Grover, if you would start, please.

Ms. GROVER. I think it is really several issues. I do think that there is a concern about morale at TSA. As was mentioned earlier, morale at DHS as a Department is very low, and morale at TSA is even lower, and that does affect people's engagement to their work. But there are weaknesses in the equipment that TSA uses in terms of its effectiveness, and there are challenges in encouraging a workforce of 45,000 people to do the job properly every day. That is just a lot of people to manage. So it is morale, it is management, it is attention to the technical specifications of the equipment. And I would like to see TSA spending less time on standing up new programs and more time on making sure that the programs that they have stood up are working properly.

Senator ERNST. That is good advice. Thank you. I appreciate that. Mr. MacLean.

Mr. MACLEAN. Well, a big problem with the Air Marshal mission is there is nothing going on, which is a good thing. There are no arrests happening; there is no casework happening. As you would get in a CBP or a Border Patrol station, you have hundreds of thousands of arrests, hundreds of drug cases happening. So the managers are busy. They have things to do. But when an Air Marshal commits an infraction, it causes a huge ripple in the water, and a lot of the local managers do not want to make a decision on something, so they wait on headquarters to make it for them.

So I think a possible solution is to put the Air Marshals underneath the purview of a pure law enforcement agency. There is a huge amount of former Border Patrol agents and CBPO officers in the Air Marshal Service, and they feel like it was when they were under the Immigration and Naturalization Service (INS). It was an agency that had conflicting missions. One was to naturalize people and then at the same time to catch and deport them. So they feel that is a problem. And because there is so little casework, so little to do—which is great because there is nobody dying, but bored managers are looking for something to do, or they are afraid to proactively take care of a situation until they get a phone call from D.C.

Senator ERNST. So you would say to separate the two programs and empower, really empower those officers to do more?

Mr. MACLEAN. Well, many Air Marshals say, "Why don't we go under the purview of Customs and Border Protection?" The facilities are already in all of the airports, and the management is already there. It could be a good transition.

It happened once before. The original Air Marshal Director had put the Air Marshal Service underneath Immigration and Customs Enforcement (ICE), and he did that because he saw the Air Marshals burning out. They were bored. You hire these high-speed, "eager beaver" guys and gals, and they get out there, and they are strapped down. So you have—it is like pressure cookers. Things happen. And he saw it. He saw it was going to be a quick burnout.

So he put them into ICE in order for them to have a better career path and go into making arrests and starting investigations.

Senator ERNST. Very interesting. I appreciate that.

And then I do want to address some of what Senator Johnson alluded to in his statements about the recent media reports that indicated the Inspector General discovered that TSA failed to identify at least 73 people employed in the industry that were flagged under terrorism-related activity codes. And according to the TSA, part of the reason for this is that the agency is not authorized to receive all of the information under current interagency watchlisting policy. I have huge concerns with that as well as I am sure most of our public does as well.

Employees are often granted special access without having gone through a thorough background check, and, Inspector General, if you could speak to that just very briefly.

Mr. ROTH. Sure. We share your concern, and your summary of what it is that we found is accurate. There is the Terrorist Identity Datamart Environment (TIDE) database. TSA by law did not have

access to some of the codes. In 2014, the Administrator asked for access but, again, it is a process that apparently is taking some time, so it is not quite there yet. But I think they are moving quickly on it.

Senator ERNST. OK. I thank you all very much for your testimony today.

Thank you, Mr. Chairman.

Chairman JOHNSON. Senator Sasse.

OPENING STATEMENT OF SENATOR SASSE

Senator SASSE. Thank you, Mr. Chairman. Thank you for all of your testimony. And, Mr. Roth, thank you for the work that you and your team do.

I wonder if you could unpack for us a little bit the structure of your organization. I think you have the largest IG office in the Executive Branch. Is that correct?

Mr. ROTH. No. I think we are No. 3.

Senator SASSE. OK. How many——

Mr. ROTH. DOD and Social Security Administration (SSA), I think.

Senator SASSE. How many employees do you have? And can you talk a little bit about the structure?

Mr. ROTH. Sure. We have approximately 700, about 670 employees all together, and it is broken functionally into an audit function as well as an investigative function. So we have about 220 criminal investigators who do sort of internal affairs work. We are the internal affairs agency for Customs and Border Protection, ICE, really the largest standing law enforcement agency in the government.

And then we have a separate section that does both inspections and audits, so we do the traditional sort of financial audits, but we do program audits, we do information technology (IT) audits. We do sort of inspections of various things, and write reports.

Senator SASSE. And can you talk about the background of your investors and auditors, how diverse their experiences are?

Mr. ROTH. They are quite diverse. Certainly our criminal investigators are individuals that either grew up in sort of the IG world or came from different other law enforcement agencies. They are trained criminal investigators—they are armed and have arrest power like any other criminal investigator, Federal criminal investigator would have.

Our auditors come from a variety of places, some within the Inspector General community, some from agencies, some from private businesses and private enterprise, all of whom are governed by sort of the GAO standards for auditing, the so-called Yellow Book.

Senator SASSE. Do you have a Red Team that reports to you?

Mr. ROTH. We do not, no. "Red Team" I think is a term of art that TSA uses to do internal testing, but we do not identify ourselves as "Red Teams."

Senator SASSE. So in my understanding, the leaked report of last week that showed that there have been 70 attempts by your investigators to smuggle weapons or improvised explosive devices or fake explosive devices onto planes, the failure rate was 67 out of 70 times, a 96-percent failure rate. The public is taking some comfort in the idea that this investigation was supposedly done by

"super terrorists," is the term that is reported in the media, from the Red Teams. So the Red Teams are not yours, and this leaked report is yours.

Mr. ROTH. Again, I cannot confirm or deny any of the specific results or the specific methodology by which we did our testing. As I said, we do not identify ourselves as Red Teams. They are auditors that we use who are members of the Inspector General's office.

Senator SASSE. I appreciate this, and I appreciate the classified briefings that you have given a number of us. I think what we hear you doing is clarifying that in your employ there are no Red Teams.

Mr. ROTH. Correct.

Senator SASSE. Do you understand how the stories are out there that says that these were Red Team Investigations?

Mr. ROTH. We do not. I was as disturbed as anyone by the fact that this information got into the media. We have done a number of classified penetration testings with absolutely no incident of leakage. We have started an investigation, a preliminary investigation of this to try to determine exactly where the source of the leak was.

Senator SASSE. Do you have any discomfort with the communication strategy of the Department that appears to be echoing these media testimonies? I will quote one from Secretary Johnson last week: "Red Team testing of the aviation security network has been part of the TSA mission for 13 years." There are indeed Red Teams at DHS. You are not going to in a non-classified setting clarify the nature of your investigation that was leaked, but I think we have heard you clearly say your employees are mostly auditors.

Mr. ROTH. That is correct.

Senator SASSE. Thank you. Last week's report was just one. Can you tell us a little bit more about the number, both classified and unclassified, of TSA DHS IG reports that you have issued since 2004?

Mr. ROTH. I cannot give you an exact number. It is approximately a dozen, is my sort of best estimate of what we have done since 2004. We did a series of penetration testings in 2011, both penetration testing to determine the security of the so-called sterile area—being able to just move into the sterile area without any sort of examination—covert testing of, carry-on luggage through the screening process. We had done penetration testing of the AIT machine, the sort of first-generation AIT machine, which is different than the ones we have done most recently, as well as penetration testing of the checked baggage process, and that report was earlier this year.

Senator SASSE. And are all of your investigations ultimately briefed to the leadership of DHS?

Mr. ROTH. Yes.

Senator SASSE. You said in testimony last month that TSA disagreed with most of your recommendations to a classified report on PreCheck, and you concluded, and I quote, "We believe this represents TSA's failure to understand the gravity of the situation." Can you explain what that means?

Mr. ROTH. Well, certainly. And, again, this is involving the PreCheck Program, that there are a number of different ways that

you can get expedited screening without actually having an application and your fee and your biometrics taken and your background sort of investigated to become a known traveler.

We found some security vulnerabilities. In fact, as a result of a number of whistleblowers, including the ones sitting to my left, some security vulnerabilities. We investigated those. We wrote reports making recommendations that would eliminate those vulnerabilities. TSA declined to take our recommendations, so we are sort of sitting at loggerheads as we speak.

Senator SASSE. Do you think it is possible that TSA could really have not understood how grave their problem was before last week's leaked report?

Mr. ROTH. It is something that we think about all the time. I mean, do they truly understand the nature of the risks that they face? Candidly, I worry about that.

Senator SASSE. I am basically out of time, but I would like to ask, Director Roering, one question for you as well. From your statement, are you saying that regular passenger screeners have no metrics that have to do with their success or failure rate at interdicting weapons?

Ms. ROERING. That is correct.

Senator SASSE. Thank you.

Chairman JOHNSON. Thank you, Senator Sasse. Senator Ayotte.

OPENING STATEMENT OF SENATOR AYOTTE

Senator AYOTTE. I want to thank the Chairman, and I want to thank all of you for being here.

I wanted to follow-up on a couple of questions. First of all, to understand that we have not been vetting the workers, the workforce against the FBI database. And then as I understood you, Mr. Roth, saying that, in fact, we still are not able to fully do that because of actually an access code issue. Could you let us know more about this? Because I have to say, I think all of us are quite shocked by this in terms of just basic common sense of we use the FBI background checks on people who deal with the public in a variety of contexts, and to not in this context just seems kind of mind-boggling that that step would not have been in place already.

Mr. ROTH. To do this, a little context on what lists we are discussing. There is sort of the large list, the Terrorist Identities Datamart Environment, which has information of individuals that is both verified and unverified. So it is the broader list from which gets called sort of the so-called terrorist watchlist.

So what TSA did not have access to is certain codes within that larger environment. Again, some of this information is non-substantiated. Once TSA realized, I think around 2014, that they did not have this information, Director Pistole or Administrator Pistole signed a letter asking for that, and it is now sort of in that interagency environment in order to do it.

We were able to, in the course of our audit, run 900,000 names against the TIDE database. So as we sit now, I think we have some comfort and understanding what that environment looks like; in other words, the 73 individuals we believe is the sort of sum entirety of what was missed. We gave those names to TSA as soon

as we discovered them, and I think they are following up on each of those.

So, I mean, to the extent that there was a vulnerability, I believe it has been closed, but it certainly gives you pause that this situation was allowed to continue.

Senator AYOTTE. It does give you pause because it really only takes one versus 73 in this context, and as we sit here, even the fact that there is still a bureaucratic step that is not being expedited with this request being made by Director Pistole already in 2014, I just cannot imagine that the FBI would not have moved on this with the most haste that they could possibly move, given especially your recent undercover findings. So I think that is something we should follow-up on just as a matter of bureaucracy cannot hold this up when it comes to basic vetting that needs to be done.

I also wanted to follow-up on the managed inclusion, what is being done with that, and I was interested also to see Director Roering refer to it as that PreCheck is being given out like Halloween candy in your written testimony. I think all of us think that PreCheck is a very important program for the public and access, but to the extent we do have a category of individuals that has grown exponentially, that is being used that may not go through the entire vetting process, if you could share with us what you are able to share here what you think would be better in terms of some reforms to focus the PreCheck process properly so that we really are allowing the members of the public to use it that should and still maintaining a thorough vetting of the individuals we should.

Mr. ROTH. The basic principle behind PreCheck is great because it is sort of this idea that if you are a known traveler, we have to spend less time on you than your unknown traveler, so really bringing PreCheck back to its basic form, which is we know who you are.

We wrote this report. We have briefed Members of Congress. There is proposed legislation in the House of Representatives called the "Secure and Expedited Screening Act," H.R. 2127, which basically directs TSA to bring it back to what it used to be, which is somebody looks at you and knows that you are a trusted traveler as opposed to some of these risk rules that they now apply.

Senator AYOTTE. I also wanted to follow-up—we heard a lot of discussion today about the vetting process, but one thing—because I also serve as the Chair of the Aviation Subcommittee that has been an issue—is the SIDA badges and wanting to fully understand from all of you your perspective on TSA's role in issuing SIDA badges. Many of them are not being kept track of, and that responsibility is left to the local airports.

What would you assess in terms of this issue? Is that a potential vulnerability? And what recommendations do you have on that front? That is to whoever would like to answer it.

Ms. GROVER. Sure. Well, so let me just start by saying that it is the airport's responsibility, and there are mechanisms that they have in place at the airport level to do regular checks with each of their contractors to make sure that the badges can be accounted for, and I believe that there is a trigger, like a 5-percent trigger, if a certain number of the badges have been lost, then they would

all be reissued. So there are some controls in place, but I think that it is an issue that warrants additional attention.

Mr. ROTH. We are doing some work on that, given sort of the news that has been recently out there——

Senator AYOTTE. We have had some other incidences with the SIDA badges of deep concern.

Mr. ROTH. We are doing field work right now with regard to that, sort of being able to actually go to the sites and figure out whether or not the airport authorities are appropriately and properly accounting for the SIDA badges, whether or not TSA is doing their oversight responsibility in a prudent way, and, frankly, doing some testing to see whether or not we can piggyback into secure areas and those kinds of things.

Senator AYOTTE. Thank you.

Ms. ROERING. We also conduct tests where we will call the airport and report that an employee has been terminated to determine how quickly they turn off the access according to the badges. That was a special emphasis inspection activity that we did recently. While we found a couple of challenges, in most cases when the badge was reported as lost or missing, the airport did turn off the access associated with the badge.

Senator AYOTTE. Right. I thank all of you for being here. This is an important topic. And let me just say to Chairman Johnson's point, certainly the TSA agents that I interact with in Manchester on a regular basis, I think they are very hard working, and so putting together the right process for the people who are trying to do this job effectively every day and making sure that they have our support I think is important, and then also ensuring that those agents that are doing well are empowered to do their job, I think that is part of our function here as well. So thank you all.

Chairman JOHNSON. Thank you, Senator Ayotte. Senator McCaskill.

OPENING STATEMENT OF SENATOR MCCASKILL

Senator MCCASKILL. Thank you.

You have no evidence right now that shows that contracted TSA is either cheaper or better, correct?

Mr. ROTH. I do not, no.

Senator MCCASKILL. OK. And you are not aware of any that exist?

Mr. ROTH. Correct.

Senator MCCASKILL. The magnetometer versus AIT, do we have numbers, good numbers, on the cost to operate and speed of use on those two different devices?

Mr. ROTH. We have not done any work in that area. I know that TSA itself has some metrics with regard to that, but I do not have that available.

Senator MCCASKILL. Well, I feel like I am handcuffed because we do not have TSA here. I will request it from TSA if it is available. It is very obvious to me, because I am always looking for AIT, because I have a knee. So I either get somebody to touch me a lot, or I do AIT. I am TSA Pre. So even though you do not know this unless you start asking, I go through the TSA Pre line, and then I ask them to go over to the AIT machine.

Now, it is catch-as-catch-can at airports. Some airports immediately accommodate you. Others say, "No, you cannot do that." And then when you get there—every airport is a little different. It is like snowflakes. Some of them say that you get to leave your shoes on and everything in when you go through the other line, if you have your TSA preboarding pass with you. Others are no. So, it is kind of a mess. But I do not really care as long as I get to go through this instead of this.

And about 50 percent of the time, they have the AIT shut down, and I have to ask for them to open it. And so they may have one sitting there. Now, some airports do not even have one sitting there. It was not until very recently they even had one at the Southwest terminal at Reagan.

So I am curious if your work has focused on this, and maybe the Marshal can speak to this, too. Why are we not keeping those AIT machines going all the time at every facility? Because we spend a lot of money on them, and I know this is the whole thing of time versus safety and how quickly can we move people through, right? Is that what it is?

Ms. ROERING. Yes, you have hit the essence of the problem. It is much faster to expedite people through a metal detector than an AIT, but this is better security than going through a metal detector. A metal detector will not detect a nonmetallic IED, which is one of the biggest threats to aviation security.

Senator MCCASKILL. Think of all the first-time travelers with knees and hips that are going through that magnetometer that do not know how much time they are going to save and how much time TSA is going to save if they go through the AIT instead, if they were to ask like I ask. I am worried that they are letting me use it because in some of the airports I am in, especially at home, they know who I am. And, that is really wrong. Anybody with a hip or knee ought to be told they should go through the AIT to save time and money—and, of course, be more safe. So I want to keep following up on this magnetometer.

Now, why can't we have more AIT machines? Well, because we are cutting the budget. So we have to remember, as we all sit and pound the desk about how bad TSA is, we keep cutting the amount of money they have. And we ask them to do more and do it better. Clearly, one of the issues is, in fact, resources and how many people are working. The times I have gotten into difficult conversations with people at the airports about why the AIT is not open, they just say, "We do not have the staff. It takes more staff to run it, and we just do not have the staff to run it." So I think that is also an issue.

The Marshals. Are you saying now, Mr. MacLean, that they are not preboarding, the Marshals? Have they changed that?

Mr. MACLEAN. It is hit or miss. It depends on where they are flying from. One thing they all tell me is that when they fly from international origins, they are paraded by the foreign agents.

Senator MCCASKILL. I still see them preboarding. I mean, it is pretty obvious who they are.

Mr. MACLEAN. Well, the way it should be done is they should be boarding with the passengers, and——

Senator MCCASKILL. By the way, isn't that better security also, because aren't they commingling with the passengers, with more opportunities, with eyes and ears——

Mr. MACLEAN. Absolutely.

Senator MCCASKILL [continuing]. To figure out who there might be on that plane that might be a problem?

Mr. MACLEAN. Correct.

Senator MCCASKILL. When they roll up at the beginning of boarding and they go on, clearly they are not physically impaired, clearly they are not traveling with small children. Now, they are not in uniform, but usually they are in jeans, and then they are sitting in strategic places on the airplane when you get on.

So I do not understand why—is this something that anybody can speak to? Why do they think it is a good idea to put these people on ahead of time?

Mr. MACLEAN. We cannot dictate what the foreign countries can do.

Senator MCCASKILL. No, but this is here in the United States.

Mr. MACLEAN. I am not aware of that. I understand that that problem has been—that the Air Marshals have the option, 100 percent option to board with the passengers. But most of the Air Marshals now are flying long routes to places where they are mandating preboarding. So the janitors see them. The workers on the front line——

Senator MCCASKILL. I see them on my plane, and typically the planes I am going on are not longer than a 2-hour flight, and they are getting on ahead of time.

Mr. MACLEAN. That is a problem.

Senator MCCASKILL. Is that their option?

Mr. MACLEAN. Yes, it is. As far as I am concerned——

Senator MCCASKILL. Why can it be their option? Should they not be required to stand in line with everybody else and commingle?

Mr. MACLEAN. I would like that, absolutely. And also at the same time they could be gauging suspicious activity.

Senator MCCASKILL. Right. If you want them walking around the airport, a perfect place to walk around the airport and be among the airport is waiting in line with all the passengers.

Mr. MACLEAN. Correct.

Senator MCCASKILL. Is there a reason that they are being given the option? Do you know, Ms. Roering, since TSA is not here? Ms. Grover or Mr. Roth?

Ms. ROERING. I do not have an answer to that, but we could ask to find out and get back to you.

Senator MCCASKILL. I mean, it is more convenient for them to get on first. It is nice not to have to wait. You do not have to get—especially if you are doing Southwest——

Mr. MACLEAN. I can only speculate, but it is possible that the Air Marshals may not want to lose their overhead bin space.

Senator MCCASKILL. Exactly. Just like all of us.

Mr. MACLEAN. I am just speculating.

Senator MCCASKILL. Yes, especially when you are traveling an airline like Southwest, which I fly frequently. Being at the front of the line——

Mr. MACLEAN. Well, Southwest Airlines, it is a free-for-all, for the most part.

Senator MCCASKILL. Correct. But I bet we could figure out with Southwest how they could make sure that they have some seats at the front.

Mr. MACLEAN. That all depends on how smart the flight attendants are going to run that operation.

Senator MCCASKILL. OK. Well, I want to stay on the contractor versus employee. I need to talk to Mr. Dodaro about this, but it seems to me that you all ought to start putting in the audit from GAO, the budget for the year of which you are doing the work compared to the previous years. I think everyone needs to understand that there is a price to be paid for us continuing to cut and cut and cut the domestic side of Homeland Security, the domestic side of our national protection. It is a problem that we are seeing this year again that we are going to create a $40 billion slush fund in the Department of Defense, but yet we are going to shortchange port security, airport security, cybersecurity, the Central Intelligence Agency (CIA), FBI, all in the name of holding on to an ill-conceived sequestration number. So I think you guys should think about doing that.

Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you, Senator McCaskill. When we are talking about resourcing, I do have to throw out the word "prioritization," so we need to look at priority of spending. You can also rest assured this will just be the first in a series of hearings on TSA.

Senator MCCASKILL. So I will get a chance at TSA?

Chairman JOHNSON. Yes, and we can talk about Boarding Group B on Southwest Airlines for folks. Senator Baldwin.

OPENING STATEMENT OF SENATOR BALDWIN

Senator BALDWIN. Thank you, Mr. Chairman. I very much appreciate your holding this very valuable hearing.

I also want to thank the witnesses and especially our whistleblower witnesses for being here to share your stories and your experience. And a special thanks to Ms. Roering. You raised the alarm on inadequate PreCheck background checks, and as you are stationed at the Minneapolis-St. Paul International Airport where, as the Chairman and I know, many of our constituents fly in and out of on their way to other destinations, we appreciate your leadership.

I wanted to follow-up on a line of questioning that some of the previous Senators went down with Mr. Roth just so I understand it very specifically.

With regard to TSA access to the terrorism-related information in these databases and, in particular, the lack of access to certain codes, I thought I heard you say earlier that there was a statutory impediment. And then you indicated that it is in the process of being worked out bureaucratically between agencies. And I want some clarity for our Committee as to whether we need to see legislation on this pushed through in an expedited fashion or whether this is on the verge of being resolved between agencies.

Mr. ROTH. Thank you for that question, and my apologies for the confusion. As I understand the process, it is sort of an administrative process that is done within the government itself. There is not a need for legislation.

Senator BALDWIN. OK.

Mr. ROTH. I think the access to that information is generally governed by statute, but it does not require a statutory fix for TSA to apply to have access to those codes, only, for example, if the Committee that decides whether or not TSA has access to the codes, for some reason refuses that access, then there may be a statutory fix that would be needed. But until that process goes all the way through, I think that is what needs to occur.

Senator BALDWIN. While I am on the topic of legislative or policy changes that we should be aware of, I think most of the testimony that I have heard points to leadership, points to management, points to following the rules that are already in place or examining that, all of which the agency would have the authority to do as it currently stands. Please highlight for me, each of you, if there is anything in your testimony that we should pay attention to that requires a statutory change. Anybody?

[No response.]

OK. Thank you.

I wanted to have you, Ms. Roering, speak a little bit further about this issue of performance metrics that are skewed toward timeliness rather than accuracy. I know you touched on this briefly in response to Senator Carper. But can you elaborate more on performance measures that track wait times and those that track the ability to detect weapons or explosives and how that affects both safety and TSO performance?

Ms. ROERING. Thank you for the question, Senator Baldwin. When there is an excessive wait time, which by definition for TSA is currently over 20 minutes in a regular lane and 5 minutes in a PreCheck lane, there is immediate reporting required through our coordination centers to the regional offices and ultimately to headquarters. That report requires a thorough analysis of the individual number of TSOs that were out for training or called off sick and scheduled absences. There is just a lot of focus and a lot of information that is needed to be gathered when we have excessive wait times.

In terms of our monthly testing, which is conducted by my inspectors, we brief the FSD basically once a month on the results of the tests. There is no metric associated with it. The test results are shared among screening management, but, quite honestly, there is just no metric to focus on the detection rates and whether or not that would reflect badly on the FSD's scorecard.

Senator BALDWIN. Mr. MacLean, you have brought to our attention a lot of information about the threat of IEDs, and certainly given the failed bombing attack of the Shoe Bomber and the Underwear Bomber and these sort of things, the evolving ability of terrorists to assemble miniature IEDs and remotely detonate them or, as you described, the increased threat of larger IEDs in the airport perimeter are huge concerns.

You have already commented a little bit further in the questioning, but how do you believe resources should be reprioritize to

better protect against these threats? And if you could elaborate a little bit more about the VIPR Teams that you were talking about earlier in that capacity to help address this threat.

Mr. MACLEAN. I am glad you asked that because I really want to talk about it.

Once again, if the PreCheck is done well, it reduces the time that the screeners need to focus on non-threatening passengers. So I would like to see those TSOs participate more on VIPR Teams, and then the four points that I mentioned on the physical security implementation on the aircraft so that you can get more Air Marshals on the ground into those VIPR Teams.

I love that thought of—and these are not teams that I want down there ripping and arresting anybody that they see. This is purely trying to build rapport from the local authorities all the way down to janitors and cooks. For instance, you might have a cook that sees something every day, the same thing, but one time he reported it to his boss, who might be some knucklehead who just says, "I do not have time for this. You are not a cop. Quit playing cop. I have better things to do." So he is frustrated. So, he does not go—he barely speaks English. He does not want to go forward with it. But if there is that uniform VIPR guy who has built a rapport with him, asks him about his family, is very interested in what he sees every day, he might come to him for something that is out of the ordinary, and that little thing just may be that IED that Air Marshals are scared to death to be stuck flying with.

Senator BALDWIN. Thank you.

Chairman JOHNSON. Thank you, Senator Baldwin. Senator Lankford.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. I thank all of you for your work on this. Millions of Americans fly every day, and they are very dependent on what is happening with TSA and the security and what you all are also bringing to the table both from whistleblowing and from doing basic inspections. So I appreciate what you are doing to be able to help out the American people in this. It is extremely important.

Let me run through just a couple different questions here.

Mr. Roth, you have in your testimony that you "have repeatedly found that human error—often a simple failure to follow protocol—poses significant vulnerabilities." What do you attribute that to? Is that systemic? Is that training? Is that management? Is that morale? Where is that coming from?

Mr. ROTH. I would say it is all of the above, Senator. I think it does involve training, it does involve morale, it does involve management. You have an enormously large distributed workforce. But you are right; it is one of these things that you have to follow the SOP every time. If you do not, that is where we find the vulnerabilities.

Senator LANKFORD. OK. So there are all kinds of accountability built into the system for time and efficiency. You were talking about that before. So if you go past 5 minutes in PreCheck or past 20 minutes in the regular line, there are all kinds of accountability. But is there the same kind of accountability structure built in for someone that is not following protocol?

Mr. ROTH. I am not aware of that. I will leave it to the other witnesses.

Senator LANKFORD. Have other folks seen that? Or has the standard really become a time-based standard at this point?

Ms. ROERING. It is a time-based standard, but if our TSOs do not follow SOP, the agency treats that as a conduct issue versus a performance issue, which, again, impacts the morale.

Senator LANKFORD. Sure. And TSA agents and what is happening in the Department of Homeland Security on the whole has just been terrible morale on the whole. These are great folks, and the people that I have traveled back and forth with in Oklahoma City, where I catch a flight every single week, are terrific folks and extremely friendly, very engaged. They understand the value of what is going on. They are great folks. But the morale seems to continue to come in time and time again bad. That does not help us as the traveling public.

Let me go through a couple things here as well. Mr. Roth, also, there have been ongoing issues with procurement with TSA, both getting equipment that is outdated, getting the wrong equipment, getting too much equipment that is stored in a warehouse, and this has been an ongoing problem. Is it getting better?

Mr. ROTH. It is hard to determine that at this point. Certainly, the kinds of work that we have been doing shows that this is a continual problem. We just did a report, for example, with regard to TSA maintenance contracts where it is about a $1.2 billion set of contracts over the course of 4 years in which TSA does not have the ability to understand whether or not routine maintenance is, in fact, being performed, or whether they are being billed for things that actually occurred.

Senator LANKFORD. So basic sustainment.

Mr. ROTH. Correct.

Senator LANKFORD. OK. So what is happening on the procurement side? Because there are lots of folks that are vendors that are rushing into this space now because they know there is a very large market when something is purchased. Is there a good standard of improvement there to say this piece of equipment is 2 percent better? Is that enough to be a multi-million to multi-billion-dollar contract? How are the standards for procurement coming out to try to increase our effectiveness?

Mr. ROTH. Certainly DHS-wide this is one of the emphasis areas of the Secretary. He is trying to professionalize the acquisition process within DHS. TSA is obviously part of that. I cannot speak to sort of how it is working on current acquisition projects, but it is something that, frankly remains a challenge.

I will say, for example, the AIT machines, that is a single vendor, so there is no real competition in the market for what is a very significant capital purchase.

Senator LANKFORD. OK. We have had a lot of conversation this morning about PreCheck and about how in PreCheck you have a million people that have gone through that process of PreCheck, what was the number? 7 million people that are now basically authorized to go through it at some point through other different variations.

Do we need to change the name from "PreCheck" to something else? Because we have a large number of people that are really not being prechecked. They are just being expedited through this process. Am I getting that correct?

Ms. GROVER. Yes, sir. That is correct, and particularly for people who are selected at the airport, these are not individuals who were previously identified as low risk. And so TSA's premise is that they are providing real-time threat assessment through the use of Behavior Detection Officers and explosives detection. But we have raised concerns about the lack of effectiveness data on the BDOs, and during the time of our review, we found that TSA was not consistently using the explosive trace detection as their protocols called for. So there is a need for more attention to that.

Senator LANKFORD. If I remember the report correctly from reading through it—and you can correct me on this if I get it wrong—basically when they were evaluated for behavioral detection, it did not come out any different than just random chance did.

Ms. GROVER. Yes, sir, that is right.

Senator LANKFORD. OK. Well, that is not really PreCheck at that point. It is difficult to call the line a PreCheck line when there is really a no-check portion of it where part of it has gone through—they have done a thorough vetting process and part of it is just random chance that they are going through it. So my understanding is this is a faster process because they have done a more thorough background than this one.

Mr. MacLean, I understand what you were saying before. There is great benefit to be able to help separate, as you said before, to be able to blow some of the hay off the stack so it is easier to find the needle. I get that completely. But we cannot call it "PreCheck" if it is really no-check and PreCheck combined.

Mr. MACLEAN. Well, I will tell you, you are familiar with Secure Electronic Network for Travelers Rapid Inspection (SENTRI)?

Senator LANKFORD. Yes.

Mr. MACLEAN. I know a Border Patrol agent, active duty, who applied for SENTRI. He got denied because when he was a juvenile, he got into a fight, and he cannot have a SENTRI pass. So it may be some things are just not being put together and implemented right.

Senator LANKFORD. Right.

Mr. MACLEAN. But I love the program just because——

Senator LANKFORD. Well, no, I am good with the program on it because it is a reasonable thing, because there are a lot of Americans that are regular fliers, they want to go through that, they want to go through the vetting, and to be able to go through the line that is a faster line in a PreCheck-type line. My statement is: If it is PreCheck, let us really have it prechecked. If they are a Trusted Traveler, I have no problem with that, because there are high standards for that. If they are active-duty military, I have no problem with that. But if we have folks that are just randomly coming to the airport and they say, "You do not look like a terrorist, so I am going to put you over there," that is not really PreCheck at that point. We have another line for that. And we need to be able to evaluate that as well.

There are 73 people—and I know others have already talked about this as well—73 folks that the IG reported were—that their code was related to terrorism. I would assume that means they are on the no-fly list. These were individuals that TSA had allowed to go through the system as employees kind of behind the perimeter there.

Mr. ROTH. They would not necessarily be on the no-fly list. The TIDE list is a very sort of broad list of terrorist identities, some of which is verified and some of which is not verified. The no-fly list is a subsection of that TIDE list.

Senator LANKFORD. OK, of that larger list.

Mr. ROTH. Yes.

Senator LANKFORD. That is going to be corrected where there is access now, and how quickly can that be corrected where that record can be tied into TSA and so they can have access to be able to look at both?

Mr. ROTH. I do not have that information with me. I know that the specific 73 names we did report back to TSA, and they are taking action on those folks.

Senator LANKFORD. But we do not have an idea at this point how fast they could take action on that, just to be able to do it as a follow-up?

Mr. ROTH. I am sorry. I do not.

Senator LANKFORD. OK. We will follow-up on that in the days ahead and find out the speed of that and so we can be able to sync all those lists together. Thank you.

Chairman JOHNSON. Thank you, Senator Lankford.

Just a quick follow-up on that. Inspector General Roth, you are saying we do not need legislation, that the authority already exists, that it is just a matter of will to do it?

Mr. ROTH. That is my understanding.

Chairman JOHNSON. OK. I want, to a certain extent, to summarize some of the things we have heard. We are really basically trying to detect two things: either explosives or weapons. The failure with the AITs, obviously we put those in place to try and detect explosives because metal detectors do not. And so we use the AITs, and now weapons are getting through.

Wouldn't a pretty simple solution be either two views through the AIT—I do not want to discuss exactly where the failure is, but, a frontal and a side view, as well as put a metal detector on the other side. That would be a relatively simple solution that would certainly increase our rate of detection. Is that not true?

Mr. ROTH. I would assume it would be for weapons.

Chairman JOHNSON. OK. That leaves us with explosives. What work has been done in terms of bomb-sniffing dogs? I have read some things. I do not have it right now that I can cite. Bomb-sniffing dogs are extremely effective. Can anybody speak to that? Mr. MacLean, you are shaking your head.

Mr. MACLEAN. I worked at a Border Patrol checkpoint. I was blown away with what a dog can sense. I have seen heroin wrapped in coffee, duct tape, Saran Wrap, hermetically sealed, and then dunked in a tank of gasoline, and the tank sealed and secured, and the dog still hits on it.

So if they can do that with drugs, if they can do that with bombs, they are amazing. They are amazing creatures.

Chairman JOHNSON. Ms. Roering.

Ms. ROERING. Currently, the regulatory program has oversight for the passenger screening canine program, and I have witnessed at various locations the use of a decoy where an individual would be carrying an explosive in a backpack or on their person, and in every case the dog was able to detect the explosive and also very favorable results with that program.

Chairman JOHNSON. Ms. Grover.

Ms. GROVER. Yes, sir, TSA has about 800 canine teams total now, and they have been found to be effective. They are expensive.

Chairman JOHNSON. Well, so is the $7.2 billion we are expending on, again, security theater.

Ms. GROVER. Yes, sir.

Chairman JOHNSON. Again, let me be clear: I think security theater to a great extent does deter. I think we need, as Mr. MacLean was talking about, layered defense. We need to think outside the box. We have to think smarter. And so from my standpoint, if you have a very high percentage in terms of effectiveness of a bomb-sniffing dog, I think that solution is pretty obvious, isn't it?

Inspector General Roth, can you speak to that?

Mr. ROTH. I think it is important for TSA to look at all options and to figure out exactly what is going to work, but try different things. This reliance on cutting-edge technology clearly has its challenges to it, so I would agree with you that they need to start to look at other things as well.

Chairman JOHNSON. I mean, isn't part of the problem as Americans we watch movies and we always have a silver bullet technological solution, and we are finding out that these technological solutions are failing at a very high rate. And so maybe we need to step back a little bit and go, well, what actually works. Again, I would argue a bomb-sniffing dog, they may be expensive, but if we are not 100 percent effective, think of how expensive that will be.

Ms. Grover, do you know exactly how expensive are these units? Have you done a study on that? Can you illuminate the Committee on that?

Ms. GROVER. So I believe that the startup costs are about $100,000 for the conventional canines and in the neighborhood of $220,000 for the passenger screening canines (PSC), and then an annual cost thereafter of about $60,000 a year for the conventional canines and about $160,000 a year for the PSC canine teams.

Chairman JOHNSON. So I would really love to have the GAO provide us a report that takes those costs, multiplies those times the number of teams we actually have to have pretty full coverage in U.S. airports.

Mr. MacLean, you look like you are chomping at the bit here.

Mr. MACLEAN. Well, remember, every canine comes with an officer——

Chairman JOHNSON. Precisely.

Mr. MACLEAN [continuing]. Who has a keen sense of feeling people out, reading faces, building rapport. Sometimes having a dog with you, people approach you or you become more approachable.

Chairman JOHNSON. Again, my point is what we are doing clearly is not working, and so we have to think outside the box and look for a different solution.

Mr. MacLean, I do want to give you the opportunity, because you were not able to tell your story of whistleblowing, and I really do want you to tell your story and how you were retaliated against, because that has been a problem that I have seen repeatedly now in my 4 years of people that have the courage in the Federal Government, coming forward, telling a story that has to be told, and then they are retaliated against, which has a very chilling effect on those individuals that we do need to come forward. So, please, take this opportunity to tell your story.

Mr. MACLEAN. Well, in July 2003, it kind of accidentally fell into my lap. After a lot of problems with us preboarding before the passengers, having to wear somewhat of a uniform to get on every flight, we were brought in for an unprecedented emergency suicidal al-Qaeda terrorist hijack emergency briefing, and we were all told that in any moment we were going to be under attack, and the flight deck was going to be breached, and those aircraft were going to be flown into east coast United States targets and European capitals.

Just 2 days afterwards, all Air Marshals got an unsecured text message sent to their unsecured phone instead of their encrypted smartphones, a message that we want everyone to avoid late cancellation fees, therefore, we need to have everyone cancel their hotel rooms indefinitely.

Later on, the GAO and the Inspector General discovered that that was going to be the plan until the new fiscal year. So for 60 days or longer, any aircraft that was going to fly 4 hours or longer was not going to have an Air Marshal team on them.

First of all, we thought it was sort of a test. We get this text message that made no sense to us 2 days after this emergency briefing, so I just wanted to confirm it with the supervisor, and the supervisor told me, he goes, "We have run out of money, and we are going to have to fly puddle jumpers until something happens."

Chairman JOHNSON. This occurred when? When did this briefing——

Mr. MACLEAN. Late July 2008.

Chairman JOHNSON. OK.

Mr. MACLEAN. So afterwards I called the Inspector General hotline, and I got routed to two other offices——

Chairman JOHNSON. We need to stand in recess for this Committee hearing. Apparently, the Capitol Police is clearing this so—we should be locked down and stay in place?

OK. We are clearing the floors. So if you could in an orderly fashion please exit as quickly as possible. Thank you.

[Recess.]

I would like to gavel this hearing back in.

It is unfortunate what happened here as we were concluding this hearing. A threat was called in. In today's world, we have to take those threats very seriously.

I want to commend the Capitol Police for acting responsibly and swiftly. We cleared the hearing room. We cleared the floor. Fortunately, the threat was determined to be false.

But, again, that is the world we live in today. It is very unfortunate.

Suffice it to say that this is going to be the first in a series of hearings in terms of the challenge that the TSA has in trying to really succeed in its dual mission of keeping this Nation safe, identifying every possible threat, preventing those things from harming any American, and at the same time allowing efficient throughput so that Americans do not wait excessively in lines and do not miss flights or any form of transportation.

So we will continue to explore this. I will continue to work with Secretary Jeh Johnson. I will continue to work with the new TSA Administrator, Vice Admiral Neffenger, and ask those gentlemen to think outside the box, take a look at the priorities that we need to establish in terms of being most effective and most efficient at providing the kind of security and traveling convenience that we possibly can within the TSA.

So with that, the hearing record will remain open for 15 days, until June 24 at 5 p.m., for the submission of statements and questions for the record.

This hearing is adjourned.

[Whereupon, at 1:33 p.m., the Committee was adjourned.]

APPENDIX

Opening Statement of Chairman Ron Johnson

"Oversight of the Transportation Security Administration: First-Hand and Government Watchdog Accounts of Agency Challenges"

June 9, 2015

As prepared for delivery:

Good morning and welcome.

Today's hearing will shed light on some of the problems within the Transportation Security Administration. TSA is charged with protecting the traveling public's safety by screening passengers and baggage as well as securing our nation's transportation network.

Recent media accounts and reports issued by the Government Accountability Office and the Department of Homeland Security Office of Inspector General have identified numerous problems within the agency that raise questions about whether TSA is effectively fulfilling its mission. Specifically, serious questions have been raised about potential mismanagement, wasteful procedures, retaliation against whistleblowers, low morale and security gaps within TSA. These matters are troubling and must be addressed.

In February 2015, news reports revealed that 1,400 security badges were lost by or stolen from employees at the Hartsfield-Jackson Atlanta International Airport over a two-year span. In March 2015, authorities arrested two TSA contractors for conspiracy to smuggle methamphetamines through the San Francisco International Airport. On June 1, 2015, news broke about a DHS OIG investigation that used undercover auditors, known as "Red Teams," to test security weaknesses in airport screening by smuggling weapons or simulated explosives through security checkpoints. According to media reports, TSA failed 95 percent of the time to prevent the Red Teams from successfully smuggling prohibited items. Today, GAO and the inspector general will be able to offer more information about the problems they have uncovered while auditing or investigating TSA.

We will also hear from two current TSA employees with first-hand accounts about problems within the agency. Federal Air Marshal Robert MacLean will testify about challenges in aviation security and the Federal Air Marshal Service. Assistant Federal Security Director for TSA at the Minneapolis-St. Paul International Airport Rebecca Roering will testify about TSA's PreCheck program and screening deficiencies.

TSA is charged with the vital duty of securing this country's transportation systems. As the committee considers the nomination for the next administrator of TSA, these issues are critical to understanding what actions need to be taken at the agency. I thank the witnesses for their willingness to provide their knowledge and expertise on these important issues, and I look forward to their testimony.

###

Statement of Ranking Member Thomas R. Carper
"Oversight of the Transportation Security Administration: First-Hand and Government Watchdog Accounts of Agency Challenges"
June 9, 2015

As prepared for delivery:

I thank the Chairman for holding this important and timely hearing.

Few federal agencies interact with the American people more on a daily basis than the Transportation Security Administration. The men and women who work for TSA have a very difficult, but extremely important job.

Last month, I spoke on the Senate floor about two women who have dedicated their careers to keeping our aviation system secure by working for TSA. In fact, one of these women was shot in the line of duty and showed up to work, the very next day. Every day, these women and their colleagues around the country work in a very challenging environment to keep our aviation system – and those of us who use it – safe and secure. We don't do enough to acknowledge that and to thank them when they do their jobs well.

While I believe it is important for us to recognize exemplary performance when it is done at TSA or throughout other parts of the Department of Homeland Security more often than we do, this committee also has an obligation to exercise our oversight responsibilities when performance falls well short of that standard.

Thanks to our witnesses before us today, we have been alerted to a number of instances where performance by TSA and its employees appears to have been disappointing and, even, troubling. Just yesterday, for example, we learned from the DHS Inspector General that seventy-three individuals with possible links to terrorism have been granted credentials to access secure areas of airports across our country.

And last week, of course, we learned about significant vulnerabilities at passenger screening checkpoints uncovered by the Inspector General. The reported failure rates for detecting prohibited items at checkpoints are more than troubling. They are unacceptable. I look forward to reviewing the DHS Inspector General's full report and recommendations later this summer. That said, I am encouraged by the swift action taken by the Secretary of Homeland Security to address the Inspector General's findings.

Since 2011, the Transportation Security Administration has transitioned from a 'one-size-fits-all' screening philosophy to one that is more risk-based. This approach is designed to allow TSA to deploy its limited resources to the areas where we face the greatest threat.

However, as the Inspector General and GAO have identified, such a swift transition may have created vulnerabilities in the system. Given recent reports, it is more important than ever for the Transportation Security Administration to have a permanent, Senate-confirmed leader in place. I thank the Chairman and his staff for working so quickly and cooperatively with my staff to move Vice Admiral Neffenger's nomination, which we'll examine in a hearing tomorrow.

With that, I look forward to the testimony and thank the witnesses for appearing here today. I am especially grateful that current front line employees have joined us today to discuss their perspective on how to improve TSA.

###

Statement of Jason Harrington

June 9, 2015

I worked for the Transportation Security Administration as a TSO from 2007-2013, and as the senior writer for O'Hare airport's TSA newsletter in 2011. Although the agency's knee-jerk response to criticism from any given former employee is that said employee's concerns are outdated, the fact of the matter is there are perennial problems within the organization that have existed from the beginning, and which still plague the agency to this day. As a writer and blogger, many current TSA agents regularly contact me to discuss their concerns with the organization. The most commonly cited concerns among floor-level employees are as follows: 1) A lack of a consistent, agency-wide strategy in addressing the inherent dilemma of security needs versus the need to process passengers as quickly as possible so as to avoid flight delays 2) Poor management culture 3) A questionable promotion system and 4) An unwieldy and inefficient SOP and recertification system.

The recent failure of agents to detect 95% of covert Red Team tests is the most prominent issue facing the agency right now, and several current agents have agreed with me that the greatest challenge when it comes to such failures stems from the fundamental catch-22 of the TSA's mission: if agents properly perform SOP down to the last detail, then internal testing results will improve and flyers will be safer. But meticulous adherence to the TSA's SOPs, such as they are, will mean that lines will back up to the ticketing counters, and people won't be able to fly. Flights will be missed due to the enormous security delays, and the distended passenger lines themselves will become choice terrorist targets. It's a classic quantity versus quality dilemma. This push-pull between security needs and commercial pressure is one of the many reasons agents are likely to fail covert testing. An effective solution for reconciling these two conflicting demands will be crucial in any effort to improve the organization. I have heard hundreds of speeches from TSA managers ordering agents to follow SOP in the name of national security or else face termination, and then, just hours later, heard the very same managers shouting at agents to disregard the SOP in the name of reducing passenger wait-times.

Managers who play this duplicitous game are common. Poor management has for years been one of the most widespread complaints among front-line TSA workers, and remains so today. To be fair, there are many good managers at TSA. One of the qualities of a good manager is that he or she acknowledges the aforementioned quantity versus quality dilemma, and makes best efforts to operate with an even-handed, transparent, *Realpolitik* approach. But the bad managers, as any front-line TSA agent will tell you, far outnumber the good. In talking recently to several current TSOs, the same time-honored complaints regarding TSA management came up.

There are far too many TSA managers who reign with a tyrannical hand, and whose promotion to a managerial position remains a mystery to the workforce. Many managers have high school diplomas and no real security or leadership experience prior to TSA, while their subordinates have advanced degrees, security and managerial experience, and yet are somehow overlooked for promotion time after time. There's a lot of talent on the screening floor, but the vast majority of that talent goes un-utilized. The promotion system is rife with cronyism, and fraternization

between managers and floor-level employees is extremely common. In my time I saw a manager who did not know what the word "nocturnal" meant when reading through a fellow officer's doctor's note involving work restrictions; another had to ask his subordinates how to spell the word "entry." Still another manager was arrested after attempting to evade Chicago-area police. The incident was well-publicized, and an account of the story appeared in a local newspaper. Drugs were found on the manager's acquaintance. Yet the manager was back on the floor within a few days, and received little more than a routine write-up. Managers are consistently more concerned about whether or not officers are chewing gum or have an acceptable hair color than whether or not the officers are treating the traveling public with respect or operating in a way conducive to real security. TSOs are so on guard from toxic management that it is hard for them to focus on their jobs.

The most extreme example of macro-level mismanagement, as well as misuse of funds, that I ever witnessed occurred in March of 2012. It still nicely encapsulates the ethos of TSA culture today, as confirmed by my private discussions with agents currently on the floor. In 2012 a blogger named Jonathan Corbett released a video proving that anyone could bypass the full-body radiation scanners in place at the time. Corbett filmed himself repeatedly passing through the scanners with a medium-sized metal object— the equivalent, for all intents and purposes, of a gun. He provided proof to the public that the machines could easily be rendered useless by exploiting a laughable weakness in the technology: metal items on passengers' bodies showed up as black on TSA officers' screens, but the background of the image was also black, rendering guns, knives, and other metallic weapons indistinguishable from the image background to TSA scanner operators. *The TSA had paid millions of dollars for full-body scanners that couldn't detect a passenger attempting to bring a gun aboard a plane.* The Corbett video went viral, and the TSA downplayed the video's significance, while floor-level TSA employees knew that Corbett's assertions and demonstrations involving the scanners were correct. The TSA clumsily attempted to cover up the scanners' critical flaw with a panicked internal directive to us front-line TSA officers within a week of the release of the Corbett video, instructing all officers to begin patting down the sides of every fifth passenger, essentially making the machines no more than million dollar random pat-down generators, a procedural redundancy, since random pat-downs were and are already performed on passengers. Compounding this comedy of errors was the fact that the radiation scanner technology was not only ineffective, but slow, as well. Wait-times began to increase due to the radiation scanners, and so management began pressuring TSOs to speed up the floor rotation, thus violating the agency's own official privacy-safeguard procedure that was supposed to ensure that officers would never come face-to-face with the passenger whose nude image they viewed. Management often pressured agents to speed up the floor rotation under threat of disciplinary measures. It thus became simple, in many cases, for officers to match a passenger with the nude image just viewed, completely validating just one of EPIC's privacy concerns. FOIA requests for the checkpoint footage of the average large, highly trafficked airport where the backscatter machines were installed could substantiate this.

Any current TSA agent will tell you that there are also serious organizational problems involving the SOP and annual re-certification tests. There are currently 13 different SOPs related to checkpoint screening alone, including the PreCheck SOP, MI1, MI2, TDC SOP, KCM SOP, the regular checkpoint SOP, the Special Screening SOP, and the Wounded Warrior SOP. Officers

are expected to have memorized all the information from these disparate, disorganized sources, and a failure to follow any of the hundreds of pedantic points in those SOPs can lead to discipline. TSA agents are so worried about procedural trivialities that they lose sight of the big picture: securing the traveling public.

Officers should be focusing more attention on passengers, and less attention on objects. John Pistole initiated the idea of screener discretion, and TSA agents were elated. However, it didn't take long before the idea of screener discretion became hollow. Agents were able to use discretion, as long their discretion didn't fall on the wrong side of a local rule instituted by a capricious manager or supervisor. One of the things that would make the TSO position a more fulfilling job would be the ability to utilize a brand of common sense— for instance, to have the discretion to loosen special screening procedures on what is clearly a harmless passenger (say, a 50-year-old cancer patient flying with her family), so as to focus attention elsewhere.

The redundant and poorly executed recertification tests are another organizational flaw that plagues agents, both past and current. Officers are often told after taking one of the theoretical annual recertification tests that they have failed a particular portion of the test, yet there are widespread claims that the testers at times mistakenly fail officers, and at other times mistakenly pass them. I personally experienced this. There was at least one occasion when I was sure that I failed a portion of a recertification practical test, confessed to my test proctor, who was a TSA supervisor and friend of mine, that I believed I failed a portion of the test, but was then told by the test proctor not to worry about my self-confessed failure, even though I did in fact fail a portion of the pat-down procedure. Thus, I was unjustly passed. Conversely, there were other times when I, along with thousands of TSA agents, was unjustly failed during a recertification test. A more organic, holistic approach to re-certification testing would be better; one where officers were measured by their actual, CCTV-recorded, day-to-day performance on the floor, and not by a single private performance in a small room with two fellow TSA officers observing.

While an inordinate amount of time at the agency is spent fussing over pedantic procedural points, major security gaps remain open. Random, 100% officer screening is supposed to be in place at the TSA as a counterbalance to insider threats, but at O'Hare there was a period of approximately one year where I neither observed nor heard of any random employee screening, at all. At several points during my 6 years of employment, I witnessed managers warning screeners in advance when the surprise random employee screening would take place, thus defeating the entire purpose of 100% employee screening. Random drug testing was another poorly executed procedure: the supposedly random testing occurred like clockwork between the months of October and March, so that the common wisdom on the floor for all 6 years of my employment was that you only had to show up to work with clean urine for those 6 months.

I end with a quote from a current screener working at a category X airport. When I asked him what he would tell this committee if he were here right now, he asked that I simply tell you this: "When I first started after September 11, they were advertising federalization of airport security so as to put in place 'professional screeners who want to make TSA a career.' That vision never manifested. No one wants to make TSA a career."

In all my time as a TSA screener, I only ever met two people who claimed to like working for the TSA, and who expressed a desire to make it a lifetime career. I am sad to report that my friend's comment is reflective of a larger truth among the TSA workforce: the thing the average TSA agent wants most is to get out of the TSA. This contributes to a vicious circle: the TSA is always desperate to hire anyone, and thus, a lot of unqualified people end up in decision-making positions, making the TSA work environment even more toxic and less attractive as a career path. Perhaps the greatest security vulnerability at the nation's airports stems from the cold truth that the easiest way for a potential terrorist to bypass TSA security would be to put in an application to be a TSA officer.

STATEMENT OF JOHN ROTH

INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

UNITED STATES SENATE

CONCERNING

OVERSIGHT OF THE TRANSPORTATION SECURITY ADMINISTRATION: FIRST-HAND AND GOVERNMENT WATCHDOG ACCOUNTS OF AGENCY CHALLENGES

June 9, 2015

Chairman Johnson, Ranking Member Carper, and Members of the Committee: thank you for inviting me here today to discuss the challenges at the Transportation Security Administration that the Office of Inspector General has uncovered in our numerous audits and evaluations of TSA.

Whistleblowers

Before discussing TSA's challenges, I would like to acknowledge the TSA whistleblowers that I join on this panel today. Being a whistleblower is seen to be hazardous in the Federal Government, and we are gratified when TSA employees – as well as employees from other DHS components – are willing to step forward to identify problems within the agency. Whistleblower disclosures can save lives as well as taxpayer dollars, and whistleblowers play a crucial role in keeping our Department efficient and accountable.

Our office can only investigate that which we know about, and whistleblowers serve as the IG's eyes and ears. We have been able to successfully complete a number of audits, inspections and investigations as a result of information we have received from whistleblowers. We review over 16,000 complaints – more than 300 per week – to better understand and respond to potential waste, fraud, and abuse in the Department's programs and operations.

Whistleblowers perform an important public service by reporting evidence of wrongdoing, and they should never be retaliated against for doing so. Pursuant to the *Whistleblower Protection Enhancement Act of 2012*, the DHS OIG has established a Whistleblower Ombudsman to educate Department employees about prohibitions on retaliation for whistleblowing, as well as employees' rights and remedies if anyone retaliates against them for making a protected disclosure.

Whistleblowers' identities are protected by the *Inspector General Act*, which prevents the OIG from disclosing the identity of an employee who provides information or a complaint without the employee's consent. Whistleblowers may anonymously or confidentially provide information to the DHS OIG through the toll-free Hotline or the public facing website or the Whistleblower Protection Ombudsman.

The TSA Mission

TSA's mission—to protect the Nation's transportation systems to ensure freedom of movement for people and commerce—is incredibly difficult. First, it is a massive operation, with a budget of more than $7.2 billion in

fiscal year (FY) 2015. Each day, TSA screens about 1.8 million passengers and about 3 million carry-on bags at 450 airports nationwide. Second, we face a classic asymmetric threat in attempting to secure our transportation security: TSA cannot afford to miss a single, genuine threat without potentially catastrophic consequences, yet a terrorist only needs to get it right once. TSA's 50,000 transportation security officers (TSO) spend long hours performing tedious tasks that require constant vigilance. Complacency can be a huge detriment to TSA's ability to carry out its mission. Ensuring consistency across DHS' largest workforce would challenge even the best organization.

Unfortunately, although nearly 14 years have passed since TSA's inception, we remain deeply concerned about its ability to execute its important mission. Since 2004, we have published more than 115 audit and inspection reports about TSA's programs and operations. We have issued hundreds of recommendations to attempt to improve TSA's efficiency and effectiveness.

- We have conducted a series of covert penetration tests—essentially testing TSA's ability to stop us from bringing simulated explosives and weapons through checkpoints, as well as testing whether we could enter secured areas through other means. We identified vulnerabilities caused by human and technology-based failures. Although the results of those tests are classified, I welcome the opportunity to brief the Members of this Committee regarding our findings in the appropriate closed setting.

- We have audited and reported on TSA's acquisitions. Our audit results show that TSA faces significant challenges in contracting for goods and services. Despite spending billions on aviation security technology, our testing of certain systems has revealed no resulting improvement.

- We have examined the performance of TSA's workforce, which is largely a function of who is hired and how they are trained and managed. Our audits have repeatedly found that human error—often a simple failure to follow protocol—poses significant vulnerabilities.

- We have looked at how TSA plans for, buys, deploys, and maintains its equipment and have found challenges at every step in the process. These weaknesses have a real and negative impact on transportation security as well.

My testimony today will focus on the vulnerabilities and challenges identified by our more recent work on passenger and baggage screening, access controls to secured areas, workforce integrity, and TSA's operations.

Passenger and Baggage Screening

Risk Assessment Rules

We applaud TSA's efforts to use risk-based passenger screening because it allows TSA to focus on high-risk or unknown passengers instead of known, vetted passengers who pose less risk to aviation security. However, we have deep concerns about some of TSA's decisions about this risk. For example, we recently assessed the PreCheck initiative, which is used at about 125 airports to identify low-risk passengers for expedited airport checkpoint screening.

Since 2012, TSA has massively increased the use of PreCheck, allowing expedited screening for nearly half of the flying public. TSA did so in four ways:

- Granted PreCheck eligibility to other Federal Government-vetted or known flying populations, such as those in the CBP Trusted Traveler Program.
- Established and increased the PreCheck application program, which requires individualized security threat assessment vetting.
- Implemented risk assessment rules.
- Used "managed inclusion" for the general public, allowing random passengers access to PreCheck lanes without having assessed their risk.

As a result of our inspection, we concluded that the first two methods are sound approaches to increasing the PreCheck population, but the latter two create security vulnerabilities. Based on our review, we believe TSA needs to modify the initiative's vetting and screening processes. We also determined that PreCheck communication and coordination need improvement. TSA did not concur with the majority of our 17 recommendations; we believe this represents TSA's failure to understand the gravity of the situation. (*Security Enhancements Needed to the TSA PreCheck Initiative, (Unclassified Summary) OIG-15-29*)

As an example of PreCheck's vulnerabilities, we recently reported that, through risk assessment rules, a felon was granted expedited screening through PreCheck. The traveler was a former member of a domestic terrorist group and, while a member, was involved in numerous felonious criminal activities that led to arrest and conviction. After serving a multiple-year sentence, the traveler was released from prison.

The traveler was sufficiently notorious that a TSO recognized the traveler, based on media coverage. In scanning the traveler's boarding pass, the TSO received notification that the traveler was PreCheck eligible. The TSO, aware of the traveler's disqualifying criminal convictions, notified his supervisor who directed him to take no further action and allow the traveler to proceed through the PreCheck lane.

TSA agreed to modify its standard operating procedures to clarify TSOs' and supervisory TSOs' authority in referring passengers with PreCheck boarding passes to standard screening lanes when they believe it is warranted. However, TSA disagreed with our recommendation regarding the Secure Flight program. The failure to implement this recommendation perpetuates a security vulnerability. (*Allegation of Granting Expedited Screening through TSA PreCheck Improperly (Redacted) OIG-15-45*)

We are pleased that bipartisan legislation has been introduced in the House of Representatives to address this issue. The legislation, known as the *Securing Expedited Screening Act* (H.R. 2127), would direct the TSA to make expedited screening available only to individuals who are vetted PreCheck participants and to people TSA identifies as known-risk and low-risk, such as those enrolled in CBP's Global Entry program or other DHS trusted traveler programs. We support this legislation and believe it represents an important step forward in transportation security.

Passenger and Baggage Screening

Detection of dangerous items on people and in baggage requires reliable equipment with effective technology, as well as well-trained and alert TSOs who understand and consistently follow established procedures and exercise good judgment. We believe there are vulnerabilities in TSA's screening operations, caused by a combination of technology failures and human error. Since 2004, we have conducted eight covert penetration testing audits on passenger and baggage screening operations. Because these audits involved covert testing and contain classified or Sensitive Security Information, we can only discuss the results in general terms at this hearing. However, we have recently briefed Committee staff about

our testing in the appropriate closed setting, and we are available to brief Committee Members at your convenience.

One penetration testing audit identified vulnerabilities in TSA's use of Advanced Imaging Technology (AIT) equipment[1] at domestic airports. TSA acknowledged that it could improve operation of new passenger screening technologies to prevent individuals with threat objects from entering airport secure areas undetected and agreed to take the necessary steps to increase AIT's effectiveness. (*TSA Penetration Testing of Advanced Imaging Technology (Unclassified Summary), OIG 12-06*)

In September 2014, we reported the classified results of our tests of checked baggage screening. We also reported that TSA did not have a process to assess the causes of equipment-based test failures or the capability to independently evaluate whether deployed explosive detection systems were operating at the correct detection standards. According to TSA, since 2009, it had spent $540 million for checked baggage screening equipment and $11 million for training. Despite that investment, TSA had not improved checked baggage screening since our 2009 report on the same issue. (*Vulnerabilities Exist in TSA's Checked Baggage Screening Operations (Unclassified Summary), OIG-14-142*)

We have recently completed the fieldwork regarding covert penetration testing to evaluate the effectiveness of TSA's Automated Target Recognition software[2] and checkpoint screener performance in identifying and resolving potential security threats at airport checkpoints. The specific result of our covert testing, like the testing we have done in the past, is classified at the Secret level. We will be issuing our final report to the Secretary and Congress in late summer or early fall.

TSA uses layers of security to prevent dangerous items or individuals from entering aircraft. In one layer, TSA uses behavior detection officers to identify passenger behaviors that may indicate stress, fear, or deception. This program, Screening Passengers by Observation Techniques (SPOT), includes more than 2,800 employees and has cost taxpayers about $878 million from FYs 2007 through 2012.

---

[1] AIT equipment screens passengers for metallic and nonmetallic threats, including weapons, explosives, and other objects concealed under layers of clothing, without physical contact.

[2] Automated Target Recognition software is designed to enhance passenger privacy by eliminating passenger-specific images and instead auto-detecting potential threats and highlighting their location on a generic outline that is identical for all passengers.

In 2013, we audited the SPOT program and found that TSA could not ensure that passengers were screened objectively. Nor could it show that the program was cost effective or merited expansion. Further, in a November 2013 report on the program, the Government Accountability Office (GAO) reported that TSA risked funding activities that had not been determined to be effective. Specifically, according to its analysis of more than 400 studies, GAO concluded that SPOT program behavioral indicators might not be effective in identifying people who might pose a risk to aviation security. TSA has taken steps to implement our recommendations and improve the program. However, the program remains an example of a questionable investment in security. (*Transportation Security Administration's Screening of Passengers by Observation Techniques (Redacted), OIG-13-91*)

Access Controls to Secure Areas and Workforce Integrity

Airport employees, as well as unauthorized individuals, entering the secure areas of airports, pose a serious potential risk to security. Controlling access to secured airport areas is critical to the safety of passengers and aircraft. Despite TSA's efforts to ensure only cleared individuals enter secure areas, we have identified numerous vulnerabilities.

Airport Badges and Access to Secure Areas

We recently reported on TSA's controls over the vetting of aviation workers who apply for credentials allowing unescorted access to secured airport areas. We reviewed TSA's process for vetting workers for terrorist links, criminal history, and lawful status. We also sought to determine the accuracy and reliability of data TSA uses for vetting.

We concluded:

- TSA has multiple, layered controls for vetting workers for terrorism, and its process is generally effective. However, TSA could not identify all individuals on the Consolidated Terrorist Watchlist because current interagency watchlisting policy does not authorize TSA to receive all terrorism-related categories of information. We identified 73 individuals with possible terrorism-related information that was not reported to TSA. TSA acknowledged that these individuals were cleared for access to secure airport areas despite representing a potential security threat.

- TSA lacks effective controls for vetting applicant's criminal history and work authorization. TSA relies on individual airports for criminal history and work authorization checks. Presently, TSA does not have an adequate monitoring process in place to ensure that airport operators properly adjudicated credential applicants' criminal histories.

- Moreover, law and FBI policy generally prohibit TSA and the airports to conduct recurrent criminal history vetting and rely on individuals to self-report disqualifying crimes. TSA is planning a pilot program for late 2015 whereby the FBI will begin providing automated updated from the FBI for new criminal history matches associated with individuals who have undergone prior criminal history records checks.

- With respect to work authorization vetting, TSA data indicates that airports may not be consistently verifying that credential applicants possess the immigration status necessary to work in the U.S.

- Finally, we identified thousands of aviation worker records that appeared to have incomplete or inaccurate biographic information, including incomplete names, passport numbers, alien registration numbers, Social Security Numbers, and aliases. TSA has taken steps to address some of these weaknesses, and enhancements should become effective within 2 years.

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

The issues that we identified are consistent with prior reports. In February 2013, we identified problems with TSA's Aviation Channeling Services Provider project, which uses vendors to relay airport badge applicants' biographical information and fingerprints to TSA for vetting. Because TSA did not properly plan, manage, or implement the project, airports nationwide experienced a backlog of background checks. To address the backlog, TSA temporarily allowed airports to issue badges without the required background checks. Consequently, at least five airports granted badges to individuals with criminal records, giving them access to secure airport areas. In response to our findings, TSA agreed to develop a lessons learned report, establish a policy requiring all projects to include a comprehensive plan, communicate customer service expectations to vendors and monitor their performance for accountability, and require inspectors to review badges issued without

the required background checks. (*Transportation Security Administration's Aviation Channeling Services Provider Project, OIG-13-42*)

We also used covert testing to determine whether unauthorized and potentially dangerous individuals could gain access to secured airport areas. In addition, during this audit, we identified the extent to which TSOs, airport employees, aircraft operators, and contractors were complying with related Federal aviation security requirements. Our test results are classified and cannot be discussed here today, but we can say that we identified significant access control vulnerabilities and recommended improvements. (*Covert Testing of Access Controls to Secured Airport Areas, OIG-12-26*)

In response to congressional concerns and media reports about missing badges, which could allow unauthorized people access to secure airport areas, we very recently began a review of TSA's controls over access badges. We intend to identify and test TSA's efforts to mitigate the risks of unaccounted for, lost, stolen, or terminated airport-issued badges.

Workforce Integrity

The integrity of TSA's workforce is also an important factor in the safety of our airports, as well as the public's trust in TSA's handling of their personal belongings. Although only a small percentage of TSA employees have committed crimes or engaged in other egregious misconduct, even a few publicized cases of wrongdoing can affect the public's confidence and potentially undermine deterrence.

Some of these crimes are serious. For example, we investigated a TSO who conspired with members of the public in a scheme to smuggle Brazilian nationals through an international airport. For his role in the crime, the TSO was sentenced to 10 months' incarceration, followed by 36 months of supervised release.

In another case, a supervisory TSO was convicted for assisting a drug trafficking organization responsible for smuggling large quantities of narcotics through an airport. With the supervisory TSO's assistance, the organization bypassed security with the narcotics and passed them to couriers on the secure side of the airport for transport to the United States. The TSO was sentenced to 87 months of imprisonment and 2 years supervised release.

TSA Operations and Management Oversight

We have continuing concerns with TSA's stewardship of taxpayer dollars spent on aviation security.

Acquiring and Maintaining Equipment

Over the years, TSA has made significant investments in acquiring and maintaining passenger and baggage screening equipment, including Explosives Detection System machines, Explosives Trace Detection machines, AIT machines, Bottled Liquid Scanners, x-ray machines, and walkthrough metal detectors, yet a series of our audits found issues with TSA's acquisition management.

We conducted an audit of TSA's methods for planning, deploying, and using AIT machines at airports. We found that the component did not develop a comprehensive deployment strategy for this equipment. TSA also did not require program offices to prepare strategic acquisition or deployment plans for new technology that aligned with the overall needs and goals of its passenger screening program. As a result, despite spending approximately $150 million on AIT units, TSA continued to screen the majority of passengers with walkthrough metal detectors. Without documented, approved, comprehensive plans and accurate data on the use of AIT, TSA was unable to effectively deploy this new technology where it was needed and, instead, relied on walkthrough metal detectors to screen the majority of passengers. By doing so, TSA potentially reduced the technology's security benefits and may have inefficiently used resources to purchase and deploy the units. (*Transportation Security Administration's Deployment and Use of Advanced Imaging Technology, OIG-13-120*)

Another recent audit revealed that the safety of airline passengers and aircraft could be compromised by TSA's inadequate oversight of its equipment maintenance contracts. TSA has four maintenance contracts valued at about $1.2 billion, which cover both preventive and corrective maintenance for airport screening equipment. Because TSA does not adequately oversee equipment maintenance, it cannot be assured that routine preventive maintenance is performed on thousands of screening units or that this equipment is repaired as needed, ready for operational use, and operating at its full capacity. In response to our recommendations, TSA agreed to develop, implement, and enforce policies and procedures to ensure its screening equipment is maintained as required and is fully operational while in service. (*The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program*, OIG-15-86)

Use of Criminal Investigators

Our report on TSA's Office of Inspection provides another example of TSA's lack of stewardship of taxpayer dollars. In September 2013, we reported that the Office of Inspection did not use its staff and resources efficiently to conduct cost-effective inspections, internal reviews, and covert testing. The office employed personnel classified as "criminal investigators," who received premium pay and other costly benefits, even though other employees were able to perform the same work at a substantially lower cost. Additionally, the office's quality controls were not sufficient to ensure that its work complied with accepted standards, that staff members were properly trained, and that its work was adequately reviewed. Finally, the office could not always ensure that other TSA components took action on its recommendations to improve TSA's operations. We estimated that TSA could save as much as $17.5 million in premium pay over 5 years by reclassifying criminal investigator positions to noncriminal investigator positions.

As a result of our efforts, in February of this year, the House passed the *TSA Office of Inspection Accountability Act* (H.R. 719). Among other things, this legislation requires TSA to reclassify criminal investigator positions in the Office of Inspection as noncriminal investigator positions if the individuals in those positions do not, or are not expected to, spend an average of at least 50 percent of their time performing criminal investigative duties. This legislation is now with the Senate Committee on Commerce, Science, and Transportation. (*Transportation Security Administration Office of Inspection's Efforts To Enhance Transportation Security*, OIG-13-123)

Cybersecurity

We have conducted a number of audits that highlight our concerns about TSA's management of its information technology (IT). During onsite inspections of IT systems, we found significant, repeated deficiencies in IT systems that support TSA's operations. These include insufficient physical security and access controls for numerous TSA server rooms and communication closets, failure to implement known software patches to servers, and other deviations from DHS IT policies and procedures. Collectively, these deficiencies place the confidentiality, integrity, and availability of TSA's data at risk. We are especially concerned that repeated deficiencies mean lessons learned at one airport are not being shared with other airports. (*Audit of Security Controls for DHS Information Systems at John F. Kennedy International Airport (Redacted) (Revised), OIG-15-18; Audit of Security Controls for DHS*

Information Technology Systems at Dallas/Fort Worth International Airport, OIG-14-132; Technical Security Evaluation of DHS Activities at Hartsfield Jackson Atlanta International Airport, OIG-13-104)

This month, we will begin an audit to determine whether TSA has incorporated adequate IT security controls to ensure that its Security Technology Integrated Program (STIP) equipment performs effectively and efficiently. STIP combines various technologies to perform passenger and baggage screening. Transportation security equipment includes the servers, databases, storage devices, and systems used for explosives detection, explosive trace detection, advanced X-ray and imaging, and credential authentication. We expect to publish our final report on STIP security around the end of this year.

Conclusion

TSA has taken some steps to implement our recommendations and address security vulnerabilities. Nevertheless, some problems appear to persist. TSA cannot control all risks to transportation security and unexpected threats will arise that will require TSA to improvise, but other issues are well within TSA's control. Sound planning and strategies for efficiently acquiring, using, and maintaining screening equipment that operates at full capacity to detect dangerous items, for example, would go a long way toward improving overall operations. Better training and better management of TSOs would help mitigate the effects of human error that, although never eliminated, can be reduced. Taken together, TSA's focus on its management practices and oversight of its technical assets and its workforce would help enhance security, as well as customer service, for air passengers.

Mr. Chairman, this concludes my prepared statement. I welcome any questions you or other Members of the Committee may have.

Appendix - OIG Reports Referenced in This Testimony

Security Enhancements Needed to the TSA PreCheck™ Initiative (Redacted), OIG-15-29, January 2015

Allegation of Granting Expedited Screening through TSA PreCheck Improperly (OSC File NO. DI-14-3679), OIG-15-45, March 2015

TSA Penetration Testing of Advanced Imaging Technology (Unclassified Summary), OIG 12-06, November 2011

Vulnerabilities Exist in TSA's Checked Baggage Screening Operations (Unclassified Summary), OIG-14-142, September 2014

Transportation Security Administration's Screening of Passengers by Observation Techniques (Redacted), OIG-13-91, May 2013

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

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

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

Transportation Security Administration's Deployment and Use of Advanced Imaging Technology, OIG-13-120, March 2014

The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program, OIG-15-86, May 2015

Transportation Security Administration Office of Inspection's Efforts To Enhance Transportation Security, OIG-13-123, September 2013

Audit of Security Controls for DHS Information at John F. Kennedy International Airport (Redacted) (Revised), OIG-15-18, January 16, 2015

Audit of Security Controls for DHS Information Technology Systems at Dallas/Fort Worth International Airport, OIG-14-132, September 2014

Technical Security Evaluation of DHS Activities at Hartsfield Jackson Atlanta International Airport, OIG-13-104, July 2013

STATEMENT OF BECKY ROERING

ASSISTANT FEDERAL SECURITY DIRECTOR – INSPECTIONS

TRANSPORTATION SECURITY ADMINISTRATION

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

U.S. SENATE

CONCERNING

OVERSIGHT OF THE TRANSPORATION SECURITY ADMINISTRATION: FIRST-HAND AND GOVERNMENT WATCHDOG ACCOUNTS OF AGENCY CHALLENGES

JUNE 9, 2015

Chairman Johnson, Ranking Member Carper, and Members of the Committee, thank you for inviting me here today to discuss important concerns related to the Transportation Security Administration and security at our Nation's airports.

The mission of the Transportation Security Administration is to ensure the freedom of movement for people and commerce, which is undeniably a difficult challenge. It is also the mission of the TSA to protect the traveling public against terrorist attacks. Balancing these two priorities is critical to the success of the Agency. The ability of TSA to execute its mission has been called into question by many oversight and watchdog groups.

My testimony today will focus on a number of the security concerns and agency policies that result in vulnerabilities and morale issues across our workforce.

Leadership

Over recent years, TSA has hired into leadership positions a number of former Airline Executives and others who place more emphasis on Customer Service and passenger wait times than on security and detection rates. This is demonstrated by the amount of scrutiny that is placed upon wait times by both the Regional Offices as well as TSA headquarters. Any wait time that is deemed by the agency as excessive requires immediate reporting, a thorough analysis, and corrective action. Wait times are tracked daily on a local level and are the first item listed on our daily dashboard. Conversely, the local monthly testing of our Transportation Security Officers to determine their ability to detect weapons and explosives is not associated with any performance metric. When this testing, referred to as the Aviation Screening Assessment Program (ASAP), results in a failure to detect the item, there is basic remedial training required before the Officer may return to duty. A Transportation Security Officer may never be subjected to a covert test, either by TSA, OIG, GAO, or other entity, based on the current volume of assigned tests each month, limited resources to conduct tests, and the sheer number of Security Officers. The lack of realistic testing on a regular basis leads to complacency in our workforce.

It is not until recently, actually within the past few weeks, that detection of Improvised Explosive Devices (IEDs) has become a topic of discussion in TSA. This is the direct result of covert testing at numerous airports identifying detection rates that caused great concern. I was briefed on the failure rates of a pilot program testing effort during in a classified briefing; therefore, I cannot discuss the specifics. In the briefing, TSA Leadership recognized that poor detection rates are, in part, related to the poor morale that exists across our workforce.

In addition to the pressure our Transportation Security Officers experience regarding wait times, there is also a hesitancy by some officers to resolve alarms on passengers which impacts detection rates. From my experience as a TSA Training Coordinator as well as the Acting AFSD-Screening for over 6 months, I recognize that while the Standard Operating Procedures may instruct TSOs to resolve alarms in a certain manner, they may be intimidated or fearful of physical contact with sensitive body areas. Again, with negative reports and encounters with uncooperative passengers, TSOs may understandably experience a level of discomfort when resolving certain alarms. It is important to have active oversight by STSOs and Screening Managers to ensure that the SOPs are followed consistently. In my limited experience as a role player for these types of ASAP tests, I have placed weapon parts in sensitive areas and taped simulated explosives in my upper thigh area, and, in each instance, the female TSO did detect the test items. Given time, training, and proper oversight, our TSOs will be able to detect prohibited items to include IEDs and weapon parts regardless of their location on a person or in their property.

Just last week, after pressure from the Secretary of the Department of Homeland Security and subsequent media reports related to the recent covert testing efforts and poor detection rates, TSA began a new initiative for Federal Security Directors to become actively engaged with our workforce with an emphasis on improving morale and increasing detection rates. It is critical to the success of the organization and the safety of the traveling public to continue down the path of dedicating resources to improve detection rates, and changing the culture so our TSOs do not feel pressure to sacrifice security in order to reduce wait times.

Morale

The 2014 Federal Viewpoint Survey resulted in the Department of Homeland Security receiving among the lowest ratings of any Federal Government agency, and the TSA receiving more than their fair share of low marks. The survey demonstrated that while our frontline employees feel strongly that the work they do is important, they are not valued by leadership. The job of a Transportation Security Officer is a challenging one, with a great deal of pressure and scrutiny. For example, the expectation is that a TSO working at the Ticket Document Check (TDC) position should average 12 – 13 seconds to process a passenger. That involves comparing the photograph on the identification to the passenger, scrutinizing the identification for signs of tampering, ensuring the name on the boarding pass matches the name on the identification, and finally reviewing the boarding pass for several other data points. If a TSO misses a data point, it typically results in a disciplinary action, regardless of the circumstances. A culture of fear and distrust has been created in the agency, also impacting morale and performance of employees. This is clearly documented in the results of the survey.

Morale has also suffered from the continuous realignment efforts of various departments within TSA. Our Behavior Detection Officers, FSD Staff, Transportation Security Managers, Federal Air Marshals, and now Transportation Security Inspectors have all gone through a realignment process where many positions were eliminated and pay bands downgraded. While it is important to improve efficiencies, TSA should also review the number of employees at TSA Headquarters for potential realignment opportunities, since the important work of day to day operations exists in the field rather than the Headquarters buildings.

PreCheck Risk Assessment Rules

Equally as troubling are the security gaps associated with the TSA Pre✓® program. While a risk based approach to passenger screening is essential, TSA has expanded PreCheck to large populations of passengers who have not enrolled in or paid for the program. In the fall of 2013, I expressed my concerns with the expansion of the PreCheck program to my leadership as well as the TSA Office of Inspections. I was informed that "I better watch what I said, and that my comments would be shared with the Administrator." I later reported the concerns to the Office of

Special Counsel for investigation. The allegations were substantiated by the Department of Homeland Security Inspector General in a report titled *Security Enhancements Needed to the TSA PreCheck Initiative.*

According to the report, the OIG "determined that providing TSA Pre✓®screening to certain passengers using risked-based analysis by TSA's Secure Flight Program creates a known aviation security vulnerability," as alleged in my complaint. Even after the DHS OIG asked that TSA discontinue the practice, TSA did not comply.

TSA is handing out PreCheck status like Halloween candy in an effort to expedite passengers as quickly as possible, despite the self-admitted security gaps that are being created by the process. The TSA Pre✓® enrollment program did not meet expectations in terms of volume; therefore, PreCheck rules keep expanding as a matter of efficiency even though the agency is well aware of the associated security risks. Also acknowledged in the DHS OIG report is that "internal testing results reveal that TSA Pre✓® lane threat detection rates need improvement," which is further documented in a classified report titled *Comparison through Testing Detection Rates of TSA Pre✓®and Standard Screening Lanes.*

In addition to the passengers who enrolled and paid to participate in the TSA Pre✓®program, TSA has now extended the privilege to wide populations of passengers, some based on their affinity to an organization (for example, TSA employees with Known Traveler Numbers (KTN)) and others based on a risk assessment performed during the Secure Flight system vetting process. From personal experience and documented incidents, I know that there are security gaps in the Secure Flight system that could be exploited by terrorists. This includes processes used to identify No Fly and Selectee designations in addition to the PreCheck passengers.

Based on the concerns I voiced regarding PreCheck and the associated DHS OIG reports, on April 30, 2015 The U.S. House of Representatives introduced H.R.2127 – Securing Expedited Screening Act. The intent of the bill is "To direct the Administrator of the Transportation Security Administration to limit access to expedited airport security screening at an airport security checkpoint to participants of the PreCheck program and other known low-risk passengers." This legislation that would prevent TSA from continuing the practice of risk assessment rules to assign PreCheck status to passengers. I respectfully encourage your support of the bill as it progresses.

A second method to increase the volume of passengers through the PreCheck lanes is Managed Inclusion. There are two forms of Managed Inclusion, which are MI 1 involving the use of Passenger Screening Canine (PSC) teams, and MI 2 involving randomly selecting passengers at airport screening checkpoints to use the PreCheck lane. By randomly selecting passengers, felons or others with ill intent may be permitted to use the PreCheck lane. MI 2 includes some additional security procedures for those randomly selected to receive PreCheck privileges, to include interaction with the TSA Behavior Detection Officers (BDOs) and checks for explosives. I have no data to evaluate the effectiveness of detection rates using the MI 2 procedure, as there are currently no ASAP protocols designed for that specific process, nor are there any methods to validate the effectiveness of the techniques used by the BDOs.

MI 1 includes the PSC teams conducting Real Time Threat Assessments (RTTAs) and using vapor wake techniques to detect explosives. On several occasions, I have monitored the testing of the PSC teams by using decoys with real explosives on their person or accessible property to determine the effectiveness of the process. In each occasion, the K-9 alerted to the explosive and the item was discovered. Also, during a recent discussion with Officers from the Minneapolis Airport Police Department, I learned that after the failed attack by the "Underwear Bomber," the aircraft involved in the attack was in Minneapolis for maintenance. The Officers took this as an opportunity to test the effectiveness of the K-9 teams by walking through the aircraft with no knowledge of where the IED had been located. In each instance, the K-9 alerted to the exact location or a row adjacent to where the Underwear Bomber had been seated. Although even dogs can have a bad day, these personal observations as well as feedback from my peers who currently manage the PSC program at their airports suggest a higher level of confidence with the MI 1 risk based procedures.

Insider Threat

As documented in recent reports, the Insider Threat continues to present a security concern at our nation's airports. Although some form of screening is conducted on cargo that is transported on passenger aircraft, catering supplies, checked baggage, and, of course, passengers, there are other airport employees and contractors who have access to sterile areas of the airport as well as the aircraft who are subjected to only Criminal History Record Checks and Security Threat Assessments. A specific group of employees who are typically contractors of the air carriers present a known and greater risk, based on my experience. This group has unimpeded access to aircraft, and it was discovered that some of these SIDA

badged employees who had worked at the Minneapolis-St. Paul Airport later traveled to Syria to fight for ISIL. TSA has increased the use of the Playbook team with a focus on the Insider Threat, and needs to continue to use a risk based approach when determining the best locations to deploy the Playbook teams.

Recent reports also reveal that airports have exceeded the acceptable percentage of unaccounted SIDA identification, and failed to initiate renewal processes for the badge holders. TSA is in the process of collecting data to determine the number of unaccounted SIDA badges at each of our nation's airports. This data has not been provided to the field locations, so I have no information on the unaccountable percentages or measures to address this concern.

As an Assistant Federal Security Director for Inspections, it is my responsibility to ensure airports and air carriers are in compliance with the Transportation Security Regulations, and if incidents of non-compliance occur, ensure that they are documented and corrected. If the issue continues, it is my responsibility to initiate progressive enforcement action. I am fortunate that the airports in Minnesota are generally very proactive in terms of security; however, based on conversations with my peers, many airports and air carriers are not as proactive and consider security a "cost of doing business."

At many locations, and in my experience in the past, the Federal Security Director is reluctant to initiate enforcement action against the airport or the air carriers. Last week, at a summit with my peers, I learned of several accounts were AFSDs were instructed by their FSD not to move forward with enforcement action in fear of the impact it may have on the relationship between the TSA and the airport or air carrier. A conflict of interest exists when the FSD relies upon the airport and air carrier to provide space for passenger and baggage screening, common use baggage conveyor systems, queue line space, etc. and on the other hand has overall responsibility for execution of the regulatory program.

Additionally, Transportation Security Inspectors are being used by FSDs to perform a wide range of duties not related to their core functions. Such duties include conducting Administrative Inquiries of other TSA employees, being members of Safety Action Teams, moving bins at the checkpoints, and, perhaps most egregiously, conducting quarterly audits of Universal Enrollment Facilities to determine such items as whether or not there is hand soap in the restrooms and if the staff is friendly. These audits should be done by a Contracting Officer rather than Regulatory Inspector s. This would allow TSIs more time to focus on ensuring the safety of the traveling public. DHS should reconsider the reporting

structure for our Transportation Security Inspectors to eliminate any potential conflicts, misuse of their time, and potential pressure to use verbal counseling or administrative action in lieu of Civil Penalty enforcement actions against the airport or air carrier. TSA should consider training our Finance Officers in the field as Contracting Officer Technical Representatives (COTRs) to oversee the numerous contracts that must be monitored.

Prohibited Personnel Practices

TSA uses Prohibited Personnel Practices to pressure and even force employees to resign when management wants them removed from the agency. When allegations of misconduct occur by employees in certain positions, the Federal Security Director or other leader must refer the allegations to the TSA Office of Inspection (OOI). I have personally experienced and heard of multiple instances when the Federal Security Director is selective in terms of which items will be referred to OOI, based on their relationship with the individual. If the Office of Inspection does investigate, they send Criminal Investigators to conduct investigations of even minor administrative matters. The FSD can influence the scope and direction of the investigation. During the actual investigation, the OOI teams use heavy handed tactics to intimidate the subject as well as witnesses. In my experience, I was threatened with Criminal Prosecution, and I was later informed that the OOI Investigators told at least one person that they were simply using that tactic in an attempt to get me to resign, when they had no evidence to support the allegations. They interrogate witnesses, threaten them with polygraph testing, and design questions to obtain certain predetermined answers. Witnesses are instructed to say whatever they want against the subject, and they will not be held accountable, even if they are untruthful in sworn statements. It is a waste of taxpayer dollars to use Criminal Investigators to conduct routine administrative investigations and also destroys the morale and trust of the workforce.

Another technique used by TSA Leadership to "get rid" of employees is directed reassignments. A number of employees in leadership positions who are performing at levels that Achieve Excellence or Exceed Expectations have been given a notice of directed reassignment, with no reason or explanation. They are informed that if they do not report to the new location, they will no longer be employed. This includes employees who have not signed a mobility agreement as a condition of employment. Additionally, by TSA Management using disciplinary action to correct alleged performance issues, employees are disadvantaged financially and it causes distrust in the workplace.

The practice of using Criminal Investigators to conduct routine administrative inquires is a huge waste of taxpayer dollars and causes morale issues in the agency. TSA should reduce the Criminal Investigator workforce, re-evaluate the Table of Penalties used by the Office of Professional Responsibility, and immediately discontinue the use of interrogations during routine inquiries.

Summary

I have over 25 years of Federal Government service, starting as a Federal Air Marshal with the Federal Aviation Administration Security Division, and later serving 2 years in Singapore under the umbrella of the US Embassy. I conducted Foreign Airport Assessments in Manila as Ramzi Yousef was actively plotting to blow up several U.S. aircraft departing from Southeast Asia. On the Thursday before the tragic events of 9/11, two Special Agents from the local Joint Terrorism Task Force shared with me a classified document regarding Zacarias Moussaoui, who was in custody in Minneapolis. According to the report, jihad was near, and Moussaoui was a member of a group planning to fly commercial aircraft into buildings, killing thousands. The following Tuesday, that exact thing happened, and I vowed to do what I could to ensure it never happens again. This is why I voiced my concerns regarding Secure Flight and PreCheck, initially through my chain of command and TSA Headquarters, and ultimately the Office of Special Counsel. Although the process is time consuming and extremely stressful, I refuse to give up until someone forces TSA to address these and other security concerns. That is why I agreed to testify today, despite the retaliatory actions that I may face by the Agency.

In conclusion, the culture that exists at TSA is one of fear and distrust. While TSA cannot control all the risks associated with aviation security, the Leadership of the Agency is certainly in a position to impact change. Better training and management of the workforce would result in an improvement to morale as well as detection rates. If employees feel valued and respected, the metrics will reflect this in a positive way. TSA should eliminate security gaps created by risk assessment rules in the Pre✓® program, and DHS should reconsider the reporting structure for Inspectors to avoid any conflicts.

Mr. Chairman, this concludes my prepared statement. I welcome any questions from you or other Members of the Committee.

TESTIMONY OF

ROBERT J. MACLEAN
Federal Air Marshal
Office of Law Enforcement
Federal Air Marshal Service

U.S. Transportation Security Administration
Department of Homeland Security

BEFORE

Senate Committee on Homeland Security and Governmental Affairs

ON

"Oversight of the Transportation Security Administration: First-Hand and Government Watchdog Accounts of Agency Challenges"

June 9, 2015
Washington, DC

Chairman Johnson, Ranking Member Carper, and distinguished Members of the Committee. It is a pleasure and an honor to appear before you today to speak about the serious concerns of dozens of former and current Federal Air Marshals (FAMs) who cannot risk their privacy or careers by bringing unwanted attention to themselves, and trusted me in private with concerns they believe need to be brought to the attention of their executive leadership, Congress, and the general public. I relay FAMs' concerns to you with great responsibility because I have not flown a single mission in 10 years.

The Federal Air Marshal Service promotes confidence in the nation's civil aviation system through the effective deployment of FAMs to detect, deter, and defeat hostile acts targeting U.S. air carriers, airports, passengers, and crews.

Federal Air Marshals must operate independently without backup, and rank among those federal law enforcement officers that hold the highest standard for handgun accuracy. They blend in with passengers and rely on their training, including investigative techniques, criminal terrorist behavior recognition, firearms proficiency, aircraft specific tactics, and close quarters self-defense measures to protect the flying public.

Federal Air Marshals have an ever expanding role in homeland security and work closely with other law enforcement agencies to accomplish their mission. Federal Air Marshals are assigned as Assistant Federal Security Directors for Law Enforcement at many airports nationwide to provide law enforcement coordination with airport stakeholders and other TSA components. Currently, air marshals are also staff several positions at different organizations such as the National Counterterrorism Center, the National Targeting Center, and on the Federal Bureau of Investigation's Joint Terrorism Task Forces. In addition, they are distributed among other law enforcement and homeland security liaison assignments during times of heightened alert or special national events.

Successful accomplishment of the FAM's mission is critical to civil aviation and homeland security.

Background on my whistleblower case that was decided on by the Supreme Court of the United States

On October 14, 2001, I was appointed into the first Department of Transportation / Federal Aviation Administration (FAA) Federal Air Marshal (FAM) class of 35 Federal Air Marshals (FAMs) to graduate after the September 11, 2001 attacks. Now the air marshal program is under the purview of the Department of Homeland Security (DHS) / Transportation Security Administration (TSA) / Office of Law Enforcement/Federal Air Marshal Service (FAMS). Prior to joining I was a Border Patrol Agent and a Missile and Space Systems Specialist in the Air Force.

I was removed on April 11, 2006, for the single charge of "Unauthorized Release of Sensitive Security Information (SSI)." My oral disclosure stemmed from a July 2003 unsecured, unmarked, unclassified text message sent to all FAMs government issued Nokia 3360 — instead of to their encrypted $22 million Datamaxx Group Palm Tungsten W smartphones — informing all FAMs to immediately cancel hotel reservations and call their respective field offices for new schedules. After exhausting "proper channels," I chose to make my disclosure to the most reliable, credible, and responsible journalist covering TSA and air marshal issues, former MSNBC Chief Washington Correspondent, Brock M. Meeks. Mr. Meeks told me he was in touch with bipartisan members of Congress such as Representative Hal Rogers (KY), Senator Chuck Schumer (NY), then-Senators Hillary Clinton (NY) and John Kerry (MA), and eight others who appeared on the public record to protest plans for removal of FAM protection for all flight missions that required a hotel room. All FAMs in the country received the order just two days after an emergency training in response to a confirm an Al-Qaeda terrorist group suicidal hijacking plan to crash jets into U.S. east coast and European capitals. My disclosure was retroactively marked as SSI on August 31, 2006 — three years after the fact and four months after my removal. Several weeks after my disclosure I co-founded the first Federal Air Marshal unit of the Federal Law Enforcement Officers Association (FLEOA). FLEOA is not a bargaining unit nor a union.

Part of my work with FLEOA was working with the House Committee on the Judiciary regarding the unnecessary danger placed on flying FAMs by TSA senior executives. Hazards such as mandating FAMs to wear suits and ties on all flights, exposing them boarding before the general public, and grouping them into hotels that would later advertise on their electronic marque that they had them staying. In 2005, the Committee confronted TSA with its findings and the FAMS director later went back into retirement. The final report was released to the public in May 2006 and titled, ***"In Plane [sic] Sight: Lack Of Anonymity At The Federal Air Marshal Service Compromises Aviation and National Security"***:

https://goo.gl/t60Czk

Affirming two unanimous decisions by the U.S. Court of Appeals for the Federal Circuit (Docket No. 2011-3231), on January 21, 2015, the Supreme Court (Docket No. 13-894) ruled that my disclosure was lawful under the Whistleblower Protection Act of 1989. Six associate justices joined Chief Justice John Roberts' decision. My case is still pending before the U.S. Merit Systems Protection Board (MSPB) (Docket No. SF-0752-06-0611-M-1) Western Regional Office Administrative Judge. On April 14, 2015, administrative judge Franklin M. Kang issued an order informing DHS that he may not sustain "the sole charge and specification" in his court, and "a continuation of the hearing does not appear to be necessary." Afterwards, DHS later unconditionally rescinded my removal and retroactively reinstated me. I'm currently in settlement negotiations with DHS.

Introduction

It was a sensible reaction to September 11, 2001 attacks to hire thousands of Federal Air Marshals (FAMs) and arm pilots to avert more hijackings immediately after the 9/11 attacks. Now trying to sustain a permanent tempo of armed FAMs, armed transiting non-FAM law enforcement officers, and armed Federal Flight Deck Officers (FFDOs) pilots, needs to be reevaluated. Some of the new threats we face may come from lone-wolf attackers with suicidal motives, such as the Germanwings pilot who purposely crashed a jet into a mountain.

It's now time to implement inexpensive, yet highly effective physical security measures, then take more Transportation Security Officers (TSOs) out of the screening checkpoints and deploy more FAMs on the ground to area familiarize themselves and gather human intelligence deep inside the bowels of train stations and airports.

When a thin-lined aluminum jetliner is 40,000 feet in the sky, zooming 500 miles per hour, and crowded with fuel and passengers, flight crews and their passengers are on a potential life or death battlefield. Jetliners can become weapons of mass destruction. Flying in a commercial jetliner is a very special privilege, not a right, flight crews and passengers have a right to use all means necessary to protect their lives.

PART I: LATEST EMERGING THREATS TO AVIATION SECURITY

1. **THREAT:** Miniature Improvised Explosive Devices (IEDs) smuggled onto and hidden on aircraft

   REMEDY: Reprioritize flying-Federal Air Marshal corps resources to for more of the following: Visible Intermodal Prevention and Response (VIPR) teams with local police to gather more human intelligence, Canine IED-sniff teams, and U.S. and overseas RED TEAMS

   Implement and advertise cash and immigration incentives for airport workers to report suspicious activity that may save innocent lives

TSA Pre-Check expansion and implementation of biometric identification systems with it

TSA Pre-Check program is great program that allows TSA Transportation Security Officers (TSOs) to spend more time and resources searching higher threat passengers and their luggage. The program should continue to be vastly expanded, and improved by incorporating biometric identification systems so that attackers cannot circumvent the process.

TSA must stop charging fees for such an effective program in order to encourage more applicants. I would even go so far as to have a mobile application kits for TSA officials to roam the airports in order to solicit passengers to apply for free during long layovers or delays.

More participants means less money time wasted searching low-threat passengers.

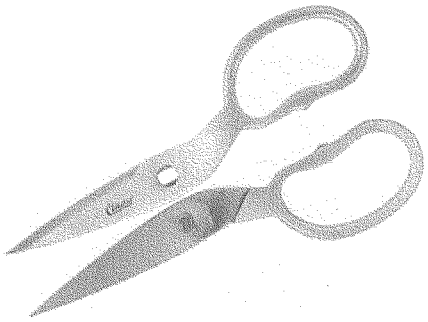
Too much focus on firearms — a distraction from looking for IEDs

Terrorist organizations, plotting mass destruction, are highly unlikely to take the risk of smuggling firearms. A terrorist organization with any common sense should have very little ambition to sneak firearms into the cabin. Reasons why:

Let's say for instance an attacker lucky enough to smuggle a semiautomatic with a 13-round magazine with a chambered round for 14 shots: an exceptionally unlikely perfect and unhindered shooter will murder 14 passengers. Once that magazine is exhausted, the weapon is useless. In comparison, an attacker armed with two 3.99-inch no-slip grip-handle blades made from a pair of TSA-approved scissors can murder a significant more amount of passengers as they never become expended like a firearm:

Scissors - *metal with pointed tips and blades shorter than 4 inches are allowed, but blades longer than 4 inches are prohibited*	NO	OK

[http://www.tsa.gov/traveler-information/prohibited-items]



http://www.shopscissors.com/chef-shear-detachable-p-294.html

Given all of the orifices in a firearm and its ammunition, it is too risky to have the gunpowder — from the ammunition — being traced by TSA officers and their machines in security. A specially made IED will most likely be hermetically sealed, more easily undetectable, and much more deadly.

A terrorist may be able to kill a handful of passengers until either he runs out of ammunition or is tackled by passengers who finally realized there were no law enforcement officers on the flight, another reason why we need a "hero passenger deputization and indemnification" law (SEE THREAT #8).

Suicide mission not necessary with current smartphone technology

With a smuggled IED and a smartphone, the need for a suicidal mission **with a firearm** is almost nonexistent. To give you an idea of how easy it is to use solid state digital devices to detonate an in-flight IED, the 20-year old Bojinka cross-Pacific Ocean commercial airliners plot was going to have IEDs detonated with common light-emitting diode alarm wrist watches.

Today, an attacker can smuggle on an IED and its state-of-the-art delay-programed smartphone detonator, hide it, disembark, and have it explode during another flight where the attacker is safe and far away.

Uniformed VIPR teams with local police as members

Like very traditional yet very effective police foot-patrols, more FAMs are needed on the ground, TSOs should spend less time searching every single passenger, and together roam individually or in teams around airport and train station properties getting familiarized with the routine operations and workers. This is where I believe uniformed VIPR teams can be very effective in area familiarization deep inside airports and train

stations, and developing rapport with transportation private sector and government workers.

Having local police officers on these teams will great increase their effectiveness because they act as ambassadors for their own departments. A concern relayed to me is VIPR teams run into chest-thumping turf wars with local authorities. Such a harmonious federal/local police team-relationship further helps with that essential need to build rapport with the local everyday workers and authorities.

It's extremely important that VIPR members have very congenial and easygoing personalities to build trusting and long relationships with workers and authorities.

Overseas RED TEAMS with canine IED-sniffers

More RED TEAM operations both in the U.S. and abroad are needed for advance searches of U.S.-flagged aircraft that overnight in foreign countries. These undercover Top Secret operatives are experienced flying FAMs who are highly trained in IED detection and disposal, and know how to test the efficiency and integrity of airport security. These teams should only report to the highest authorities.

RED TEAMS are needed in foreign countries where U.S.-flagged aircraft fly in and out of. The Christmas "Shoe Bomber" (2001) and "Underwear Bomber" (2009) came from Europe. RED TEAMS can spot and secondary suspicious passengers for more thorough searches. They also can search and sniff U.S. aircraft.

We cannot totally rely on foreign countries, especially third world, to conduct security for our aircraft due to corruption. I had foreign agent ask me to smuggle handguns into his country where they are strictly forbidden.

FAMs tell me that the foreign authorities routinely love to parade them in front of the general public and it makes their missions unbearable. Ambassador-like overseas RED TEAMS may be able to smooth over such a situation.

Vendors terminal passenger-boarding areas

Megatons of cargo not screened goes into the passenger boarding areas, i.e., magazine and newspaper stack-bundles, neck-pillows, food, beverage, condiments, cooking oil, cleaning products, etc.

Cash and immigration incentives for airport workers to report suspicious activity

Most of the people who work deep in the bowels of airports are immigrants. For many, money is not much of a motivator for them, but family unity and love is. The "If You See Something, Say Something™" campaign [
http://www.dhs.gov/see-something-say-something

] should clearly tell them the U.S. Government will immigrate their loved ones to the U.S. for stopping a commercial jet from becoming a weapon of mass destruction.

Cash motivates some people more than ethics or patriotism. The "If You See Something, Say Something™" campaign should clearly tell people that million-dollar awards are available to you for not causing the aviation security domain to collapse again like it did on 9/11/2001.

Suicide v. non-suicidal IED missions

In most of the FAMs' — who speak with me — opinions, a non-suicidal IED smuggler is more likely than a suicidal one, as many potential attackers may not want to end up in solitary confinement for the rest of their natural life like failed suicidal IED smuggler-terrorists Richard Reid, AKA: "The Shoe Bomber" of the 2001 Christmas Day-minus 3 U.S.-flagged American Airlines Flight 63, and Umar Farouk Abdulmutallab, AKA: "The Underwear Bomber" of the 2009 Christmas Day U.S.-flagged Northwest Airlines Flight 253. Another motivator to smuggle, hide, and escape from in-flight IEDs is because the vast majority may not want to die a horrible death.

This probability is good news as IED-sniff canine teams, VIPR teams, and U.S./overseas RED TEAMS may be able to search, discover, and successfully neutralize hidden IEDs with delay-switches to be detonated by terrorists who wish to live and kill again.

2. **THREAT:** Large IEDs in carry-on luggage detonated in crowded checkpoint waiting lines.

   REMEDY: Vehicle checkpoints located at airport entrances; reprioritize resources to search for IEDs; human intelligence; Canine IED-sniff teams; Cash and immigration award incentives

It's extremely easy to pack a large carry-on luggage, wait in a crowded checkpoint line, walk away the luggage, and safely detonate it seconds later.

This is a very enlightening article about exploding an IED in a crowd of passengers waiting to be screened at Denver International Airport's single-central security screening area -- much like Washington-Dulles (IAD). Former FAM, former U.S. Army commission officer Operation Iraqi Freedom veteran, and former police Special Weapons & Tactics (SWAT) operator, Jeffrey Denning, wrote this. Mr. Denning discusses how TSA's policies are a danger to aviation security on the ground:

http://jeffreydenning.blogspot.com/2009/09/terrorist-plot-prediction-airports-are.html

FAMs would be more of a deterrent and effective by proactively stopping vehicles and handling canine IED-sniffers than seated for thousands of hours in an airline chair waiting for the attacker with a firearm or knife.

3. **THREAT:** Suicidal or homicidal lone-wolf attackers or organizational terrorists infiltrating government or private sector transportation companies through employment.

   REMEDY: Human and technological intelligence gathered by law enforcement. Flight deck controls and door override from ground-control.

This is obviously a potential problem given the rogue employees willing use their position for personal gain. An example was the group of former Houston FAMs who were arrested smuggling cocaine during missions. [http://www.chron.com/news/houston-texas/article/2-ex-air-marshals-sent-to-prison-for-cocaine-1863569.php]

Flight deck controls and door override from ground-control

We will never know what truly was happening in the mind of the suicidal pilot who murdered 149 passengers by crashing Germanwings Flight 9525 Airbus A320-200 into the side of a mountain. It's impossible to read a mind, but a pattern of email, cellular, and/or social media communications may early detect an attacker's intentions. This is an argument for the Intelligence Community to responsibly analyze such digital chatter.

Another approach is to use a remote system override in which ground-control can lock or unlock a flight deck door, and also to take control of the aircraft until the threat from a pilot or flight attendant is over. FAMs tell me they are concerned that an attacker can force a flight attendant to unlock a flight deck door.

4. **THREAT:** Attacker dives into flight deck after unlocked to serve pilots or when pilots need to use the lavatory

   REMEDY: Secondary barrier gates installed in front galleys to protect the flight decks of all commercial aircraft.

These lightweight and inexpensive secondary barrier systems should be installed on all aircraft to prevent an intruder from entering the front galley when the flight deck door is opened during flight. I initially saw these ingenious devices in operation on United Airlines Premium Service Boeing 757 aircraft providing service between Los Angeles International (LAX) and San Francisco International (SFO), and New York JFK.

The device consists of a set of approximately a dozen 1/4" thick horizontal cables that quickly stretch across the entry point into the front galley. The device allows the pilots and/or flight crew enough time to secure the flight deck before a possible breach.

Every time a pilot has to open the flight deck door for food, drink, or use the lavatory, he/she risks a hijacker diving inside and recklessly taking control of the aircraft. Sometimes a flight attendant will take a drink-cart and set up a blockade of the forward area, but amped-up suicidal hijackers will just dive over unafraid of injury or death. It is worth noting that Southwest Airlines does not equip its aircraft with drink-carts.

My sources tell me that they hardly ever see these very effective cable devices on aircraft they fly on.

Here is a link to a "white paper" drafted by the Airline Pilots Association (ALPA) describing the cable secondary barrier system and recommending every aircraft be installed with one of them:

http://www.alpa.org/~/media/ALPA/Files/pdfs/news-events/white-papers/secondary-barriers.pdf

5. **THREAT:** In-flight knife attacker

   REMEDY: Equip every cabin with electric Taser devices, beanbag guns, and other non-lethal tools and assign FAMs to train flight crew members with in order to subdue attackers and defend the flight deck; equip cabin with loud high-pitched alarms; give flight deck the ability to turn off all lights; give flight deck the availability to depressurize the cabin

If I am a lone-wolf suicidal terrorist and wanted to create chaos on a plane or force it down into the ground, I would take steroids, pump iron nonstop, book a seat in first class, and board a flight with a pair of TSA-approved scissors (SEE THREAT #1)

Electrical Taser projectile weapons, rubber-bullet, and/or beanbag guns — such as the equipment used in prisons can be secured in the front galley area in the case the super-strength knife-wielding attacker tries slashing his way into the flight deck. The non-lethal weapons can be used by the flight crew or deputized passengers (SEE THREAT #7), and can be unlocked with a combination code for subsequent use. In the rare case of having a FAM team, it is dangerous have FAMs leave the "Place of Dominance" near the flight deck and walk toward the back of the aircraft, subjecting themselves to an ambush, and having their firearms and ammunition taken away from them.

The flight deck should have the capability to completely shut off all lights in the cabin to make it more difficult for attackers to cause more chaos.

Install very loud and high-pitched alarms and blinding strobe-lights in the cabin that can be turned on in order to disorient attackers or make it more difficult to communicate with other attackers.

The Captain and his First Officer can don oxygen masks and depressurize the aircraft by engaging circuit breakers located inside the flight deck. The lack of oxygen will most likely cause the terrorists to lose consciousness first as their adrenaline, breathing, and heart rates will be maximized as they carry out a suicide mission. There is the possibility that sick, elderly, or infant passengers may be left with long-term problems or death, but it is better than a gunfight between terrorists and law enforcement officers mid-flight, and/or an entire aircraft being used as another dangerous September 11, 2001 attacks missile.

6. **THREAT:** The flight deck can be penetrated, pilots attacked, and aircraft commandeered.

REMEDY: Equip every flight deck with specially modified firearms

Every flight deck should be equipped with a pre-loaded shotgun and 12-guage small-diameter pellet ammunition. The shotgun should be a modified pistol-gripped 12-guage shotgun with a shortened barrel. The 12-guage shotgun rounds should be comprised of small-diameter pellets. At close-contact range, birdshot can quickly neutralize someone trying to penetrate the flight deck. A close-contact shot can neutralize an intruder's head, heart, and/or remove a limb; a miss or partial miss will only send birdshot pellets harmlessly down the aircraft as opposed to the .40 caliber or Sig Sauer .357 ballistic rounds used by FFDOs and FAMs respectively. The shotgun should be secured with an electrical quick-release solenoid mechanism similar to the ones used in standard police patrol vehicles. A remote button or switch for the shotgun rack lock bracket can be located in a position only accessible to the Captain or First Officer.

Armed pilots are not allowed to carry their pistols on international flights due to very restrictive handgun laws, but a shotgun modified to stop one or two attackers from one foot away would be inane for a host country to deny, and risk another 9/11-style attack.

During my tenure as a U.S. Air Force Missiles & Space Systems specialist for Intercontinental Ballistic Missiles, shotgun and pellet ammunition systems were stored inside the missile silos to counter a possible attack. The shotguns would be used to defend the missiles from the attack because their pellets would not penetrate the skin of the missile and possibly ignite the rocket propellant and cause a disaster.

FAMs can provide an eight-hour or shorter course for pilots on how to ammunition-check, chamber, disengage safety, and fire the pump-action shotguns.

Russia-flagged commercial airliners have a firearm in every flight deck.

7. **THREAT:** Highly trained FAMs sitting in chairs waiting for a gun or knife attacker is a waste of valuable resources.

REMEDY: Air Marshal program should spend the vast majority of resources on training flight crews to neutralize critical incidents and local and federal law enforcement officers to be reserve/augmentee FAMs; Consideration for the Air Marshal program to be placed under the purview of DHS **Customs & Border Protection** which already has infrastructure and management in every international airport.

Streamline the FAMS into a rapid response force; and a training program for flight crewmembers and a reserve/augmentee air marshal program available to all federal AND LOCAL law enforcement officers.

Very few sharp, ambitious, and aggressive young adults aspire to sit in a chair for 25 years as an anti-terrorist law enforcement officer. I knew I would not want to do that, and the weeks after the 9/11 attacks FAA senior executives told me and other FAM applicants there's no way it would expect us to be flying FAMs 90% of our law enforcement careers. Prior to the attacks FAA FAMs spent more time training, and investigating potential aviation safety security problems than flying.

Flying air marshal duties should have been a temporary detail, not a law enforcement career: 1) The job is extremely boring and uneventful thus making FAMs lose motivation and becoming too complacent 2) The duty requiring FAMs to constantly sit idle is hard on a FAM's health 3) The constant change in time zones causes jet-lag which makes FAMs less effective.

A federal or local law enforcement officer should be able to apply for a one-year or longer temporary detail, attend a training course, finish the detail, and return to his/her prior position. The FAM overseen by the TSA should be a smaller more mobile force that only flies missions on genuine high threat flights, similar to the local police SWAT teams: FAMs should be tactically deployed on specifically threatened flights, not strategically scheduled on a large category of routes and cities threatened.

Suicidal hijackers train everyday for their single moment to simply disarm one armed passenger mid-flight; it is only a matter of time before a hijacker rushes a flight deck when its door opens mid-flight; or before a jet-lagged and unbeknownst seated FAM — experiencing inevitable complacency in his mundane profession — is ambushed, disarmed, and his/her weapon is used cause deadly chaos. FAMs experienced tremendous boredom and jet-lag, a dangerous combination. Many other dangers exists associated with traveling non-FAM armed law enforcement officers, such as not being in communication with FAMs.

<u>Unruly passengers who do not endanger the flight deck</u>

In a potential terrorist ruse, the routine of responding to unruly passengers encourages eager FAMs to impulsively engage a covert terrorist in a remote portion of an aircraft, come under attack, become disarmed, and a victim. The TSA SV Pay Band system encourages such impulsiveness because a young and eager FAM may fly

hundreds of missions without incident and is overly committed to finally getting a within SV Pay Band increase. If everyone expects the FAMs — not the passengers — to subdue unruly passengers with non-lethal force, the attacker may make his way to the flight deck. If a group of would-be attackers want to create a ruse to compel a FAM toward the back of the plane, they just need to act like unruly passengers to compel a FAM to walk into their trap and take his/her handgun away. FAMs do not lock-up their handguns someplace in the front of the plane before proceeding to subdue an unruly passenger. Despite risking punishment, poor evaluations, and/or getting black-balled from ground assignments, it is certain that some FAMs have the common sense to not follow this ridiculous expectation; but given the fact that FAMs are under a "Pay for Performance" (PFP) compensation plan, in a job they almost never effect arrests or conduct investigations, and they are trained to use these non-lethal force tools -- the temptation to finally get that increase in pay may override any common sense for an officer waiting months or years to finally make an arrest.

SV Pay Banding system is counterproductive to the FAM team thwarting threats to aviation

FAMs have a very single-dimensional job. FAMs cannot compete for PFP when they very rarely generate investigations or effect arrests. PFP has turned FAMs against each other by them filing complaints on each other for frivolous violations such as showing up the airport late, accidentally nodding off during the flight, flirting with a flight attendant, or getting into a disagreement with an airline employee, etc. FAMs are supposed to rely on each other in a team environment, but given their uneventful duties, they are only able to out-shine someone else who has petty complaints on file — this effectively disrupts the "warrior team spirit" and endangers public and national security. FAMs tell me that "FAM on FAM backstabbing" is pervasive given the fact that many of the new recruits being hired have no military or law enforcement experience.

New FAM recruits need more real-world experience

New FAM hires should have at least five years or more of combat military or law enforcement experience given they will rarely make arrests. A FAM recruit cannot have field training unit experience in this position like a municipal police officer trainee does. A municipal local police trainee rides with a highly experienced senior police officer effecting arrests all day and night long. 99% of senior FAMs have never made an arrest as a FAM.

Consideration of placing air marshal program under DHS Customs & Border Protection

The most common suggestion from FAMs is to get them out from under the purview of a regulatory and screening agency, TSA, and place them in a pure law enforcement agency that gathers intelligence and enforces the law, DHS Customs & Border Protection (CBP). CBP already has management and infrastructure in every international airport. This would also give FAMs more motivation with new diverse duties, instead of just sitting in a chair waiting for something to finally happen after

hundreds of uneventful flights. FAMs can train federal and local law enforcement officers to be surge-augmentee reserve air marshals in order to respond to specific threats, and then they go back to their departments to resume their primary duties. Other FAMs can resume high-threat international routes, be aviation security liaisons stationed overseas, become FBI Joint Terrorism Task Force members, or be on VIPR and RED teams. Such a change would not only involve FAMs in proactive intelligence and law enforcement programs, but would save taxpayers millions.

8. **THREAT:** Passengers do not attempt to restrain unruly or deadly passenger inflight incidents as they are conditioned to believe flight crews or FAMs have to respond or they're concerned about civil and criminal liability

   REMEDY: Congress and the President should pass and well publicize a law that gives flight crews and law enforcement officers the authority to deputize general passengers as Federal Air Marshals; equip every aircraft with non-lethal restraining devices; no one in the aircraft should know FAMs or any other law enforcement officers are on board, with the exception of the Captain or ground control.

Hero passenger deputization indemnification law

An unarmed 100 lbs flight attendant will not restrain a 250 lbs angry drunk or amped-up suicidal attacker. Due to a potential attacker's ruse, FAMs should no longer risk an ambush and endanger the public by walking deep into a cabin — away from the flight deck — to subdue unruly passengers. The routine of responding to unruly passengers encourages FAMs to become distracted away from the flight deck. The law needs to specifically declare that deputized passenger will be exempt from prosecution and civil liability. The flight crew can arm a deputized passenger or a group of deputized passengers with a Taser device, a non-lethal firearm, duct-tape, and/or restraints that should be standard equipment on every aircraft.

TSA Pre-Check should be used to select and screen able-bodied passengers who are willing to volunteer restraining unruly passengers. When a situation begins, ground-control can tell the flight deck if any Pre-Check-vetted passengers are on board and willing to restrain unruly passengers.

Such a law needs to be well publicized so that terrorists know FAMs will **never** leave the flight deck unprotected. The flying public also needs to know they may not be brought on criminal charges or held civilly liable for seriously injuring or killing a passenger.

When I participated in FAM training, we routinely had training scenarios with role-players. In scenarios in which the flight crew asked me to respond to an unruly passenger near the back of the plane: I did not want to endanger myself and the rest of the passengers and subject myself or my team to an ambush during a potential terrorists'

ruse, I would then deputize several passengers, and give them my hand-cuffs to subdue the unruly passenger themselves while I remain close to the flight deck. I never failed these training scenarios using this technique. It would be deemed illegal for me to deputize passengers although it was the safest action to take.

This incident involved a delusional person who concerned passengers accidentally killed as he tried to break down the flight deck door. The deceased's family sued the passengers, but the lawsuits were dismissed in light after the September 11, 2001 attacks:

http://en.wikipedia.org/wiki/Jonathan_Burton

Articles about U.S. FAMs exposing themselves mid-flight to unruly passengers as recent as last year:

http://www.csnphilly.com/article/unruly-passenger-threatens-air-marshal-flight-officials

http://www.fbi.gov/boston/press-releases/2015/haitian-national-sentenced-for-disrupting-transatlantic-flight

http://www.komonews.com/news/12934217.html

http://www.foxnews.com/story/0,2933,45298,00.html

http://www.cnn.com/2006/US/12/28/unruly.passenger/index.html

http://www.cnn.com/2008/CRIME/06/19/tsa.drunk.passenger/index.html

http://www.wtvynews4.com/news/headlines/561017.html

No one in the aircraft should know FAMs or any other law enforcement officers are on board, with the exception of the Captain or U.S. ground control

FAMs and law enforcement officers need to stop being required to informing non-essential personnel who they are, only the Captain or U.S. ground control should know.

An attacker can either view the identification procedure and ambush the FAMs or other law enforcement officers, or the attacker can threaten the life of a flight crew member to identify them.

FAMs and law enforcement officers should always be allowed to remain unidentified and board along with the passengers. FAMs in the waiting/boarding area may be able to spot suspicious activity before boarding and or take-off.

9. **THREAT**: Security Identification Display Area (SIDA) badge impostors

REMEDY: Implement biometric systems to positively identify holders; notify all employees of problem or former employees denied access to sensitive areas

When I managed the Border Patrol San Clemente, CA station northbound Interstate 5 Pre-enrolled Access Lane program (just like the Custom and Border Protection's SENTRI program at land-port entries), we not only issued applicants ID cards, but we registered applicants into an electronic fingerprint-reader and palm-reader machine databases. We were using this technology over 15 years ago, so I'm certain it has vastly improved since the 9/11 attacks. When someone quits or gets fired, all you do is click a button to deny access.

TSOs and FAMs need to be quickly informed about TSA employees being denied access to the field office or airport sterile areas. It is a problem when a distraught, disgruntled, and rogue TSA employee goes unnoticed in a sensitive area.

10. **THREAT:** "Passenger 57" movie scenario with multiple armed hijackers

REMEDY: The pilots in the flight deck can depressurize the cabin until the flight crew and passengers can take control again

In the exceptional odds of this fictional movie scenario in which a terrorist team enters the aircraft with a large cache of weapons, see **THREAT #5**.

Conclusion with regards to aviation security threats

In light of the December 22, 2001 Richard Reid IED attack on American Airlines 63, the Umar Farouk Abdulmutallab attack on Northwest flight 253, and terrorists' evolving ability to assemble miniature IEDs remotely detonated with existing handheld mobile technology, it is dangerous to not implement these relatively inexpensive but highly effective physical security measures, and put more FAMs on the ground to prevent hijackers and IEDs from boarding aircraft, instead of deploying jet-lagged FAMs to dangerously sit and wait for hijackers to attack and/or discover an in-flight IED mid-flight — when it's too late. A team of bored and sleepy FAMs sitting on **one plane** waiting for something to happen is a waste of great resources, and dangerous with current policies. More VIPR teams need to be deployed deep inside airports familiarizing themselves with the daily activity and gathering human intelligence. FAMs need to be on the ground in VIPR and U.S./overseas RED TEAMS proactively gathering and analyzing intelligence, conducting behavior detection, investigating leads, interviewing informants, and building casework that could save us from another 9/11.

Flight crews and passengers are mostly all alone high in the sky. They need to protect themselves and their flights, and the airlines and our government should seriously consider giving them indemnity laws, equipment, and training to stay alive. Flying commercial jetliners is not a right, but an **EXCEPTIONALLY SPECIAL** privilege:

https://youtu.be/uEY58fiSK8E

PART II: PERSONNEL ISSUES THAT EFFECT AVIATION SECURITY

A. **PROBLEM:** Potential whistleblowers lack of confidence in the overburdened U.S. Merit Systems Protection Board (MSPB) and its administrative judges.

REMEDY: One option: Pass a law that allows non-Intelligence Community whistleblowers to try their cases before a U.S. District Court jury.

Right now only the MSPB can review and rule on a federal whistleblower reprisal claim. This mean that only three to four administrative judges and full Board Members review a claim. One of these administrative judges is an executive agency middle manager, and the other two or three of the full Board Members are political appointees with term limits.

A U.S. District judge's salary is significantly more than an MSPB administrative judge or full Board Member, and is nominated by the U.S. President and confirmed by the U.S. Senate for life. Removing a U.S. District judge is the same process for removing the U.S. President: impeachment by the U.S. House of Representatives, and removal by the U.S. Senate.

The benefits derived by the federal government from whistleblower disclosures are measured in the billions of dollars and in other unmeasured benefits such as public safety. If a case goes to trial, there is the potential for a jury of taxpayers to determine that someone is a whistleblower or not. The MSPB does not have the resources or political independence to provide timely justice in cases where the Whistleblower Protection Act is needed most. In my own case, I would have won in 2009 instead of 2015 if I had the right to seek justice from a jury of taxpaying citizens who enjoy the privilege of flying on commercial jetliners. I risked my professional life to protect a common juror. This would have saved me some five and a half years of unnecessary emotional pain and financial desperation. As long as remedies are restricted to the administrative law system, the Whistleblower Protection Act will not be a factor when the country needs it most.

Federal Aviation Administration whistleblower Kimberly Farrington is has been waiting 18 months for her MSPB administrative judge to issue a decision after two remands from the full MSPB panel in it's Washington DC. Ms. Farrington made her whistleblower disclosures over 12 years ago. [http://www.mspb.gov/netsearch/viewdocs.aspx?docnumber=736583&version=739180&application=ACROBAT]

Federal whistleblower and retired U.S. Park Police Chief Teresa Chambers made two trips to the U.S. Court of Appeals for the Federal Circuit and three trips to the full MSPB Board in Washington DC in order to prevail after eight years. [http://www.mspb.gov/netsearch/viewdocs.aspx?docnumber=566514&version=568178&application=ACROBAT]

I can be a W-2 employee in a restaurant and report the owner for endangering public safety using spoiled meat to save on costs. If I'm terminated, laws would allow me access to a jury.

Federal laws and the U.S. Constitution allow jury access all corporate, and local and state civil services workers except the federal workforce both inside **and outside** of The Intelligence Community. A front-line non-Intelligence Community U.S. Customs & Border Protection Officer, who inspects cargo ships for nuclear devices, to a CIA Clandestine Services Operations Officer has no access to a jury.

Civil servant jury trials in cases involving classified information

If the unauthorized disclosure of SECRET or TOP SECRET classified information is a concern, a military-type courts-marshal should be established with jury members existing of agency peers who have security clearances. A presiding judge can be a senior executive, also with a security clearance, from an agency **outside** of the whistleblower's.

B. PROBLEM: The career senior executives rely too much on the TSA Chief Counsel and the political appointees for decisions on whistleblower reprisal.

REMEDY: Career senior executives would act with more independence if whistleblowers had access to jury trials; career senior executives need to be somewhat more independent of the TSA Office of Chief Counsel and political appointees.

After I told internal affairs agents and my deciding official that I was the source of the July 2003 disclosure, had no remorse, and would do it again, my deciding official, the Office of Professional Responsibility, nor TSA headquarters took any action against me for almost **five months**. Years later, the TSA Chief Counsel's office would argue that my disclosure was reckless, and I endangered countless lives and national security.

For almost five months, my deciding official chose not limit or suspend my access to classified information or my duties. He made no attempt to revoke my badge, credentials, or firearm. He would later testify that he suspected I was a protected whistleblower, but he needed the TSA Chief Counsel to make such a decision for him.

If your children's babysitter admitted to you that he molested children in the past, had no remorse, and would do it over and over again, would you let him continue to babysit for another five months while you consulted with your attorneys? No, you wouldn't.

My deciding official knew in fact I was a protected whistleblower who acted lawfully, even going so far to declare I was an "exemplary" Federal Air Marshal. Unfortunately, he was under extreme pressure by the embarrassed political appointees not to ignore their orders. After he testified in his deposition that I "didn't cause any

problems," "continued on doing the good work that [I] had been doing," "didn't cause any trouble," and suspected I should be protected, he got **demoted twice into a non-supervisory position** outside of the Federal Air Marshal Service.

The former Federal Air Marshal Service Director — in office when I won my two unanimous U.S. Court of Appeals for the Federal Circuit decisions — recently contacted me to say he was not consulted about whether or not to file the TSA's subsequent losing appeals. In 2010, this director made a sincere effort to have me reinstated, but was overruled by the TSA Office of Chief Counsel.

C. **PROBLEM:** The vast majority of Federal Air Marshals do not need expensive and time-consuming TOP SECRET security clearances.

   REMEDY: Require only U.S. Office of Personnel Management suitability certifications like Customs & Border Protection Officers and Border Patrol Agents have.

The entire time I was a FAM, I never saw a SECRET or TOP SECRET document or coversheet, nor did any FAMs tell me that they saw one except for some very rare occasions. I'm told by current FAMs that this is still the case, but that a few office-based Supervisory FAMs or acting Supervisory FAMs have access to classified material.

A Border Patrol Agent has access to land border sensor maps to give easy passage for drug smugglers, terrorists, and nuclear devices. A Customs & Border Protection Officer or can turn a blind-eye to a large shipment of illegal narcotics or a container with a nuclear device, yet neither are not required to even possess a SECRET security clearance.

The consensus is that the TOP SECRET security clearance is an easy way to fire whistleblowers. A security clearance determination has no judicial review [https://supreme.justia.com/cases/federal/us/484/518/case.html]

Former Los Angeles Federal Air Marshal Manuel "Manny" V. Alcaraz had an honorable and unblemished law enforcement record, and was beloved by his fellow coworkers. Unfortunately FAM Alcaraz angered his managers by requesting a written policy regarding a mandate to cover his visible, uncontroversial tattoos while he was detailed to conduct recurring training for other FAMs. Before being hired, FAM Alcaraz already had visible tattoos in which he disclosed during his application process and his medical entrance exam. FAM Alcaraz subsequently resigned as a trainer, causing other trainers to resign in protest. FAM Alcaraz was later accused by his managers of lying to local police, TSA investigators, and a TSA polygraph examiner about an incident in which a woman reported to police he "hit" her arm after **"stealing [her] mall parking space"** on the Saturday afternoon before Christmas Day 2007. In the local police and TSA reports of investigation, the woman changed her story to FAM Alcaraz "slapping" her arm to **"pushing"** on her arm. Local police did not obtain a warrant or arrest FAM Alcaraz, but TSA assigned two Office of Inspection Criminal Investigators to investigate.

The TSA investigators interviewed the woman's son and only one of the two third party witnesses present who stated that FAM Alcaraz "pushed" on her arm. I later interviewed that third party witness and he stated that he no longer believed FAM Alcaraz touched the woman. TSA revoked FAM Alcaraz' security clearance due to "lack of candor," and subsequently fired him for no longer having a clearance. The MSPB refused to consider the merits of the case due to Navy v. Egan, 484 U.S. 518 (1988).

In an attempt to cross-examine the accuser to present new evidence for TSA to reconsider, Mr. Alcaraz for years successfully fought his case and prevailed in a Fourth District Court of Appeal of California as his accuser attempted to avoid cross-examination by invoking state Anti-Strategic Lawsuit Against Public Participation (Anti-SLAPP) laws. But after becoming indigent, unable to find work, and spending tens of thousands in attorney fees, Mr. Alcaraz lost hope and could not afford a state jury trial to simply cross examine the woman who ended his perfect 14-year law enforcement career.

This case broke my heart, being one of the worst injustices done to an honorable law enforcement officer. This was a clear case of the security clearance revocation process being abused to settle a petty score:

> *"The victim told police she was waiting for a spot in the JC Penney parking structure when a man driving a Toyota pickup truck swooped in and stole her spot, police said."*

http://www.ocregister.com/articles/police-95586-woman-suspect.html

A report of investigation of Mr. Alcaraz' case by Nick Schwellenbach, formerly of the non-government organization, Project On Government Oversight, and now a manager in the U.S. Office of Special Counsel:

http://pogoblog.typepad.com/pogo/2010/11/why-is-the-tsa-keeping-air-marshal-employment-disputes-under-a-veil-of-secrecy.html

D. PROBLEM: The Federal Air Marshal Service has too many supervisors and managers either doing too much mundane administrative tasks or are scrounging for ways to discipline flying Federal Air Marshals (FAMs) for frivolous infractions in order to desperately justify an within SV Pay Band increase.

REMEDY: Give more administrative responsibilities to Federal Air Marshals (FAMs) and go to the General Schedule system of automatic pay increases.

FAMs are already exhausted from flying between multiple time zones. Select FAMs can be provided a secure desktop computer installed in their home and tasked with reviewing and approving travel vouchers, time and attendance sheets, special missions scheduling, and other tasks Supervisory FAMS spend much time on. Give these FAMs one or more administrative leave days a pay period to perform these duties.

Once again, there are almost no casework or arrests by FAMs, so there is very little hard positive evidence to justify within SV Pay Band increases. This motivates Supervisory FAMs to find issues to discipline jet-lagged FAMs. Place all FAMs and Supervisory FAMs on the General Schedule where they get schedules within grade increases.

This would also greatly benefit FAMs who live in high-cost of living areas as I recall a FAM who lived in Apply Valley, California and would commute up to 220 miles a day to Los Angeles International Airport. To avoid traffic, he would drive to the airport very early and sleep in his vehicle until he had to check in. This could not have been healthy for the FAM and effected his ability to thwart an attack.

Putting this solution into action and you can significantly reduce the FAMS supervisory and managerial corps.

E. **PROBLEM:** Field office managers have the discretion to make FAMs surrender their badge/credential and firearms if they are on office or airport light-duty status due to medical issues. Unarmed FAMs not only cannot defend themselves, but they cannot defend their fellow employees, family members, and the general public.

   REMEDY: A FAM's suitability to use a firearm to defend himself or others outside of an airborne aircraft should be determined by the doctor who placed him on a medical light-duty and a TSA firearms range officer.

A FAM with a broken foot may not be able to fight a suicidal attacker inside a crowded airliner up in the sky, but he may be able to draw his firearm inside a field office or elsewhere on Earth while seated, kneeling, or in a prone position to defend himself or others.

If the manager is that concerned about the FAM's condition, the manager should allow the FAM to stay home on paid administrative leave and report to the office only when absolutely needed. We should have more confidence in a winged FAM to defend us from further soft-target attacks such as those at the New Orleans International Airport on March 20, 2015 with a knife-attacker, and the fatal firearms-attacks on the Charlie Hebdo office in Paris, France on January 7, 2015, and at the Los Angeles International Airport on both July 4, 2002 and November 1, 2013.

Conclusion with regards to personnel issues

Once again, many believe that the flying-Federal Air Marshal mission should have only been a temporary detail and not become its own agency. This leads to boredom and inevitable friction between the front-line FAMs and their managers. Things go very wrong when a FAM comes back from an overseas mission in which he may have endured a parade by his foreign escorts, tolerated a curious or belligerent passenger for most of his

flight, fought through insomnia and absorbed the stress from his spouse and children about reading about another salacious news story;only later to get a voicemail to immediately see his seated and ambitious supervisor about making a mistake on a travel voucher — this is counterproductive to what the taxpayers expected in response to the 9/11 attacks.

Again, the flying-FAM mission should be temporary duty, not a career or an agency.

I'm exceptionally committed to improving aviation security so that the public has the utmost confidence, and enjoys the miracle and wonderful privilege of commercial flying. The public has a right to protect themselves when flight crew member or law enforcement officer cannot. I'm very excited and look forward to serving with the incoming TSA Administrator, Admiral Peter V. Neffenger, U.S. Coast Guard. I would be pleased to answer any questions the Committee may have.

Respectfully Submitted.

United States Government Accountability Office

GAO

Testimony
Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:30a.m. ET
Tuesday, June 9, 2015

AVIATION SECURITY

TSA Has Taken Steps to Improve Oversight of Key Programs, but Additional Actions Are Needed

Statement of Jennifer Grover, Director, Homeland Security and Justice

June 9, 2015

GAO Highlights

AVIATION SECURITY

TSA Has Taken Steps to Improve Oversight of Key Programs, but Additional Actions Are Needed

Highlights of GAO-15-678T, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

Since the attacks of September 11, 2001 exposed vulnerabilities in the nation's aviation system, billions of dollars have been spent on a wide range of programs designed to enhance aviation security. Securing commercial aviation remains a daunting task, and continuing fiscal pressure highlights the need for TSA to determine how to allocate its finite resources for the greatest impact. GAO previously reported on TSA's oversight of its aviation security programs, including the extent to which TSA has the information needed to assess the programs.

This testimony focuses on TSA's oversight of aviation security measures including, among other things (1) Secure Flight, (2) Advanced Imaging Technology, and (3) Managed Inclusion. This statement is based on reports and testimonies issued from December 2011 through May 2015. For prior work, GAO analyzed TSA documents and interviewed TSA officials, among other things.

What GAO Recommends

GAO has previously made recommendations to DHS to strengthen TSA's oversight of aviation security programs. DHS generally agreed and has actions underway to address them. Consequently, GAO is not making any new recommendations in this testimony.

View GAO-15-678T. For more information, contact Jennifer Grover at (202) 512-7141 or groverj@gao.gov.

What GAO Found

The Transportation Security Administration (TSA) has taken steps to improve oversight of Secure Flight—a passenger prescreening program that matches passenger information against watch lists and assigns each passenger a risk category—but could take further action to address screening errors. In September 2014, GAO reported that TSA lacked timely and reliable information on system matching errors—instances where Secure Flight did not identify passengers who were actual matches to watch lists. GAO recommended that TSA systematically document such errors to help TSA determine if actions can be taken to prevent similar errors from occurring. The Department of Homeland Security (DHS) concurred and has developed a mechanism to do so, but has not yet shown how it will use this information to improve system performance. In September 2014, GAO also found that screening personnel made errors in screening passengers at the checkpoint at a level consistent with their Secure Flight risk determinations and that TSA did not have a systematic process for evaluating the root causes of these errors across airports. GAO recommended that TSA develop a process for evaluating the root causes and implement corrective measures to address them. DHS concurred and has developed such a process but has not yet demonstrated implementation of corrective measures.

In March 2014, GAO found that TSA performance assessments of certain full-body scanners used to screen passengers at airports did not account for all factors affecting the systems. GAO reported that the effectiveness of Advanced Imaging Technology (AIT) systems equipped with automated target recognition software (AIT-ATR)—which displays anomalies on a generic passenger outline instead of actual passenger bodies—relied on both the technology's capability to identify potential threat items and its operators' ability to resolve them. However, GAO found that TSA did not include these factors in determining overall AIT-ATR system performance. GAO also found that TSA evaluated the technology's performance in the laboratory—a practice that does not reflect how well the technology will perform with actual human operators. In considering procurement of the next generation of AIT systems (AIT-2), GAO recommended that TSA measure system effectiveness based on the performance of both the technology and the screening personnel. DHS concurred and in January 2015 reported that it has evaluated the AIT-2 technology and screening personnel as a system but has not yet provided sufficient documentation of this effort.

In December 2014, GAO found that TSA had not tested the effectiveness of its overall Managed Inclusion process—a process to assess passenger risk in real time at the airport and provide expedited screening to certain passengers—but had plans to do so. Specifically, GAO found that TSA had tested the effectiveness of individual components of the Managed Inclusion process, such as canine teams, but had not yet tested the effectiveness of the overall process. TSA officials stated that they had plans to conduct such testing. Given that GAO has previously reported on TSA challenges testing the effectiveness of its security programs, GAO recommended that TSA ensure its planned testing of the Managed Inclusion process adhere to established evaluation design practices. DHS concurred and has plans to use a test and evaluation process for its planned testing of Managed Inclusion.

Chairman Johnson, Ranking Member Carper, and Members of the Committee:

I am pleased to be here today to discuss our past work examining the Transportation Security Administration's (TSA) oversight of its passenger and airport worker screening programs. It has been nearly 14 years since the attacks of September 11, 2001 exposed vulnerabilities in the nation's aviation system. Since then, billions of dollars have been spent on a wide range of programs designed to enhance aviation security. However, securing commercial aviation operations remains a daunting task—with hundreds of airports, thousands of aircraft, and thousands of flights daily carrying millions of passengers and pieces of carry-on and checked baggage. According to TSA, the threat to civil aviation has not diminished—underscoring the need for effective passenger and airport worker screening programs. As the fiscal pressures facing the government continue, so too does the need for TSA to determine how to allocate its finite resources to have the greatest impact on addressing threats and strengthening the effectiveness of its programs and activities. GAO previously reported on TSA's oversight of its aviation security programs, including the extent to which TSA has the information needed to assess the programs.

As requested, my testimony today focuses on TSA's oversight of four key aviation security measures:

- Secure Flight: a passenger prescreening program that matches passenger information against federal government watch lists and other information to assign each passenger to a risk category;
- Advanced Imaging Technology (AIT): a full body scanner used to screen passengers in the nation's airports;
- Managed Inclusion: a process that TSA uses to determine passengers' eligibility for expedited screening at some passenger screening checkpoints, via Pre✓™ lanes;[1] and

[1]TSA Pre✓™ is the program through which TSA designates passengers as low risk for expedited screening in advance of their arrival at the passenger screening checkpoint. Expedited screening typically includes walk-through metal detector screening and X-ray screening of the passenger's accessible property, but unlike in standard screening, travelers do not have to, among other things, remove their belts, shoes, or light outerwear. Managed Inclusion operates only at checkpoints with TSA Pre✓™ lanes.

- Aviation Workers: a program by which TSA and airports, in collaboration with the Federal Bureau of Investigation (FBI), vet applicants against the FBI's criminal history records, among other databases, and issue credentials to qualifying airport facility workers, retail employees, and airline employees, among others.

This statement is based on our reports and testimonies issued from December 2011 through May 2015 related to TSA's efforts to oversee its aviation security measures.[2] For our past work, we reviewed applicable laws, regulations, and policies as well as TSA program documents; results from AIT testing and screener performance reviews; decision memorandums; and other documents. We also visited airports—six for our Managed Inclusion work and nine for our Secure Flight work—which we selected based on a variety of factors, such as volume of passengers screened and geographic dispersion, and interviewed Department of Homeland Security (DHS), TSA, FBI officials, among other things. Further details on the scope and methodology for the previously issued reports 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

The Aviation and Transportation Security Act (ATSA) established TSA as the primary federal agency with responsibility for securing the nation's civil aviation system.[3] This responsibility includes the screening of all

[2]See GAO, *Transportation Security: Actions Needed to Address Limitations in TSA's Transportation Worker Security Threat Assessments and Growing Workload*, GAO-12-60 (Washington, D.C.: Dec. 8, 2011), *Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities*, GAO-14-159 (Washington, D.C.: Nov. 8, 2013); *Advanced Imaging Technology: TSA Needs Additional Information before Procuring Next-Generation Systems*, GAO-14-357 (Washington, D.C.: Mar. 31, 2014); *Secure Flight: TSA Should Take Additional Steps to Determine Program Effectiveness*, GAO-14-531 (Washington, D.C.: Sept. 9, 2014); *Aviation Security: Rapid Growth in Expedited Passenger Screening Highlights Need to Plan Effective Security Assessments*, GAO-15-150 (Washington, D.C.: Dec. 12, 2014); and *Aviation Security: TSA Has Taken Steps to Improve Oversight of Key Programs, but Additional Actions Are Needed*, GAO-15-559T (Washington, D.C.: May 13, 2015).

[3]Pub. L. No. 107-71, 115 Stat. 597 (2001).

passengers and property transported from and within the United States by commercial passenger aircraft.[4] In accordance with ATSA, all passengers, their accessible property, and their checked baggage are screened pursuant to TSA-established procedures at the more than 450 airports at which TSA performs, or oversees the performance of, security screening operations. These procedures generally provide, among other things, that passengers pass through security checkpoints where their person, identification documents, and accessible property, are checked by screening personnel.[5]

Secure Flight

Since its implementation, in 2009, Secure Flight has changed from a program that identifies passengers as high risk solely by matching them against federal government watch lists—primarily the No Fly List, comprised of individuals who should be precluded from boarding an aircraft, and the Selectee List, composed of individuals who should receive enhanced screening at the passenger security checkpoint—to one that uses additional lists and risk-based criteria to assign passengers to a risk category: high risk, low risk, or unknown risk.[6] In 2010, following the December 2009 attempted attack on a U.S.-bound flight, which exposed gaps in how agencies used watch lists to screen individuals, TSA began using risk-based criteria to create additional lists for Secure Flight screening. These lists are composed of high-risk passengers who may not be in the Terrorist Screening Database (TSDB), but who TSA

[4]See 49 U.S.C. § 44901. For purposes of this testimony, "commercial passenger aircraft" refers to U.S.- or foreign-flagged air carriers operating under TSA-approved security programs with regularly scheduled passenger operations to or from a U.S. airport. "Commercial aviation," as the term is used in this testimony, encompasses the transport of passengers and their property by commercial passenger aircraft as well as the airports that service such aircraft.

[5]Screening personnel include transportation security officers, and at airports participating in TSA's Screening Partnership Program, screeners employed by private companies perform this function under contract with and overseen by TSA. See 49 U.S.C. §§ 44901, 44920.

[6]The No Fly and Selectee Lists are subsets of the Terrorist Screening Database—the U.S. government's consolidated watch list of known or suspected terrorists.

has determined should be subject to enhanced screening procedures.[7] Further, in 2011, TSA began screening passengers against additional identities in the TSDB that are not included on the No Fly or Selectee Lists. In addition, as part of TSA Pre✓™, a 2011 program through which TSA designates passengers as low risk for expedited screening, TSA began screening against several new lists of preapproved low-risk travelers. TSA also began conducting TSA Pre✓™ risk assessments, an activity distinct from matching against lists that uses the Secure Flight system to assign passengers scores based upon their travel-related data, for the purpose of identifying them as low risk for a specific flight.

AIT Systems

According to TSA officials, AIT systems, also referred to as full-body scanners, provide enhanced security benefits compared with those of walk-through metal detectors by identifying nonmetallic objects and liquids. Following the deployment of AIT, the public and others raised privacy concerns because AIT systems produced images of passengers' bodies that image operators analyzed to identify objects or anomalies that could pose a threat to an aircraft or to the traveling public. To mitigate those concerns, TSA began installing automated target recognition (ATR) software on deployed AIT systems in July 2011.[8] AIT systems equipped with ATR (AIT-ATR) automatically interpret the image and display anomalies on a generic outline of a passenger instead of displaying images of actual passenger bodies. Screening officers use the generic image of a passenger to identify and resolve anomalies on-site in the presence of the passenger.

TSA's Managed Inclusion Process

TSA Pre✓™ is intended to allow TSA to devote more time and resources at the airport to screening the passengers TSA determined to be higher or unknown risk, while providing expedited screening to those passengers

[7]Standard screening typically includes passing through a walk-through metal detector or Advanced Imaging Technology system, which identifies objects or anomalies on the outside of the body, and X-ray screening for the passenger's accessible property. In general, enhanced screening includes, in addition to the procedures applied during a typical standard screening experience, a pat-down and an explosives trace detection or physical search of the interior of the passenger's accessible property, electronics, and footwear.

[8]See Pub. L. No. 112-95, § 826, 126 Stat. 11, 132-33 (2012) (codified at 49 U.S.C. § 44901(l)) (requiring, in general, that TSA ensure that all AIT systems used to screen passengers are equipped with ATR software).

determined to pose a lower risk to the aviation system. To assess whether a passenger is eligible for expedited screening, TSA considers, in general, (1) inclusion on an approved TSA Pre✓™ list of known travelers;[9] (2) results from the automated TSA Pre✓™ risk assessments of all passengers;[10] and (3) real-time threat assessments of passengers, known as Managed Inclusion, conducted at airport checkpoints. Managed Inclusion uses several layers of security, including procedures that randomly select passengers for expedited screening and a combination of behavior detection officers (BDO), who observe passengers to identify high-risk behaviors at TSA-regulated airports; passenger-screening canine teams; and explosives trace detection (ETD) devices to help ensure that passengers selected for expedited screening have not handled explosive material.

Aviation Workers Program

TSA also shares responsibility with airports to vet airport workers to ensure they do not pose a security threat. Pursuant to TSA's Aviation Workers program, TSA, in collaboration with airport operators and FBI, is to complete applicant background checks—known as security threat assessments—for airport facility workers, retail employees, and airline employees who apply for or are issued a credential for unescorted access to secure areas in U.S. airports.[11]

[9]These lists are composed of individuals whom TSA has determined to be low risk by virtue of their membership in a specific group, such as active duty military members, or based on group vetting requirements.

[10]Using these assessments, an activity distinct from watch list matching that uses the Secure Flight system to assign passengers scores based upon their travel-related data, TSA assigns passengers scores based upon information available to TSA to identify low-risk passengers eligible for expedited screening for a specific flight prior to the passengers' arrival at the airport.

[11]TSA security threat assessments include a background check to determine whether an applicant is a security risk to the United States. 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. For airport workers, TSA is responsible for both vetting and adjudicating an applicant's terrorist and immigration history while providing the results of criminal history checks to airport operators. The airport operator is responsible for adjudicating the criminal history which includes a determination of whether an applicant has committed a disqualifying criminal offense, before determining whether to issue an applicant a credential for unescorted access to secure areas of the airport. See, e.g., 49 C.F.R. §§ 1542.209, 1544.229, & 1544.230 (listing or referencing disqualifying criminal offenses).

TSA Has Taken Steps to Improve Oversight of Secure Flight, but Could Take Further Action to Measure Program Performance and Address Screening Errors

In September 2014, we reported on three issues affecting the effectiveness of TSA's Secure Flight program—(1) the need for additional performance measures to capture progress toward Secure Flight program goals, (2) Secure Flight system matching errors, and (3) mistakes screening personnel have made in implementing Secure Flight at the screening checkpoint.[12] TSA has taken steps to address these issues but additional action would improve the agency's oversight of the Secure Flight program.

Need for additional performance measures: In September 2014, we found that Secure Flight had established program goals that reflect new program functions since 2009 to identify additional types of high-risk and also low-risk passengers; however, the program performance measures in place at that time did not allow TSA to fully assess its progress toward achieving all of its goals. For example, one program goal was to accurately identify passengers on various watch lists. To assess performance toward this goal, Secure Flight collected various types of data, including the number of passengers TSA identifies as matches to high- and low-risk lists, but did not have measures to assess the extent of system matching errors—for example, the extent to which Secure Flight is missing passengers who are actual matches to these lists. We concluded that additional measures that address key performance aspects related to program goals, and that clearly identify the activities necessary to achieve goals, in accordance with the Government Performance and Results Act, would allow TSA to more fully assess progress toward its goals. Therefore, we recommended that TSA develop such measures, and ensure these measures clearly identify the activities necessary to achieve progress toward the goal. DHS concurred with our recommendation and, according to TSA officials, as of April 2015, TSA's Office of Intelligence and Analysis was evaluating its current Secure Flight performance goals and measures and determining what new performance measures should be established to fully measure progress against program goals.

Secure Flight system matching errors: In September 2014, we found that TSA lacked timely and reliable information on all known cases of Secure Flight system matching errors, meaning instances where Secure Flight did not identify passengers who were actual matches to these lists. TSA officials told us at the time of our review that when TSA receives information related to matching errors of the Secure Flight system, the

[12]GAO-14-531.

Secure Flight Match Review Board reviews this information to determine if any actions could be taken to prevent similar errors from happening again.[13] We identified instances in which the Match Review Board discussed system matching errors, investigated possible actions to address these errors, and implemented changes to strengthen system performance. However, we also found that TSA did not have readily available or complete information on the extent and causes of system matching errors. We recommended that TSA develop a mechanism to systematically document the number and causes of the Secure Flight system's matching errors, in accordance with federal internal control standards. DHS concurred with our recommendation, and as of April 2015, TSA had developed such a mechanism. However, TSA has not yet demonstrated how it will use the information to improve the performance of the Secure Flight system.

Mistakes at screening checkpoint: We also found in September 2014 that TSA had processes in place to implement Secure Flight screening determinations at airport checkpoints, but could take steps to enhance these processes. Screening personnel at passenger screening checkpoints are primarily responsible for ensuring that passengers receive a level of screening that corresponds to the level of risk determined by Secure Flight by verifying passengers' identities and identifying passengers' screening designations. To carry out this responsibility, among other steps, screening personnel are to confirm that the data included on the passenger's boarding pass and in his or her identity document (such as a driver's license) match one another, and review the passenger's boarding pass to identify his or her Secure Flight passenger screening determination. TSA information from May 2012 through February 2014 that we assessed indicates that screening personnel made errors at the checkpoint in screening passengers consistent with their Secure Flight determinations. TSA officials at five of the nine airports where we conducted interviews stated they conducted after-action reviews of such screening errors and used these reviews to take action to address the root causes of those errors. However, we found that TSA did not have a systematic process for evaluating the root causes of these screening errors across airports, which could allow TSA

[13]Secure Flight's Match Review Board—a multidepartmental entity—and associated Match Review Working Group review performance measurement results and recommend changes to improve system performance, among other things.

to identify trends across airports and target nationwide efforts to address these issues.

Officials with TSA's Office of Security Operations told us in the course of our September 2014 review that evaluating the root causes of screening errors would be helpful and stated they were in the early stages of forming a group to discuss these errors. However, TSA was not able to provide documentation of the group's membership, purpose, goals, time frames, or methodology. Therefore, we recommended in September 2014 that TSA develop a process for evaluating the root causes of screening errors at the checkpoint and then implement corrective measures to address those causes. DHS concurred with our recommendations and has developed a process for collecting and evaluating data on the root causes of screening errors. However, as of April 2015, TSA had not yet shown that the agency has implemented corrective measures to address the root causes.

TSA Performance Assessments of AIT-ATR Did Not Account for All Factors Affecting the System

In March 2014, we reported that, according to TSA officials, checkpoint security is a function of technology, people, and the processes that govern them, however we found that TSA did not include each of those factors in determining overall AIT-ATR system performance.[14] Specifically, we found that TSA evaluated the technology's performance in the laboratory to determine system effectiveness. However, laboratory test results provide important insights but do not accurately reflect how well the technology will perform in the field with actual human operators. Additionally, we found that TSA did not assess how alarms are resolved by considering how the technology, people, and processes function collectively as an entire system when determining AIT-ATR system performance. AIT-ATR system effectiveness relies on both the technology's capability to identify threat items and its operators to resolve those threat items.

At the time of our review, TSA officials agreed that it is important to analyze performance by including an evaluation of the technology, operators, and processes, and stated that TSA was planning to assess the performance of all layers of security. According to TSA, the agency conducted operational tests on the AIT-ATR system, as well as follow-on operational tests as requested by DHS's Director of Operational Test and Evaluation, but those tests were not ultimately used to assess

[14]GAO-14-357.

effectiveness of the operators' ability to resolve alarms, as stated in DHS's Director of Operational Test and Evaluation's letter of assessment on the technology. Transportation Security Laboratory officials also agreed that qualification testing conducted in a laboratory setting is not always predictive of actual performance at detecting threat items. Further, laboratory testing does not evaluate the performance of screening officers in resolving anomalies identified by the AIT-ATR system or TSA's current processes or deployment strategies.

Given that TSA was seeking to procure the second generation of AIT systems, known as AIT-2, we reported that DHS and TSA would be hampered in their ability to ensure that future AIT systems meet mission needs and perform as intended at airports unless TSA evaluated system effectiveness based on both the performance of the AIT-2 technology and screening officers who operate the technology. We recommended that TSA measure system effectiveness based on the performance of the AIT-2 technology and screening officers who operate the technology while taking into account current processes and deployment strategies. TSA concurred and reported taking steps to address this recommendation. Specifically, in January 2015, DHS stated that TSA's Office of Security Capabilities evaluated the AIT-2 technology and screening officer as a system during an operational evaluation. However, TSA has not yet provided sufficient documentation showing that this recommendation has been fully addressed.

TSA Has Not Tested the Overall Effectiveness of Its Managed Inclusion Process, But Plans to Conduct Such Testing

In December 2014, we reported that, according to TSA officials, TSA tested the security effectiveness of the individual components of the Managed Inclusion process—such as BDOs and ETD devices—before implementing Managed Inclusion, and TSA determined that each layer alone provides an effective level of security.[15] However, in our prior body of work, we identified challenges in several of the layers used in the Managed Inclusion process, raising questions regarding their effectiveness.[16] For example, in our November 2013 report on TSA's behavior detection and analysis program, we found that although TSA had taken several positive steps to validate the scientific basis and strengthen program management of its behavior detection and analysis program, TSA had not demonstrated that behavioral indicators can be used to reliably and effectively identify passengers who may pose a threat to aviation security.[17]

Further, TSA officials stated that they had not yet tested the security effectiveness of the Managed Inclusion process as it functions as a whole, as TSA had been planning for such testing over the course of the last year. TSA documentation showed that the Office of Security Capabilities recommended in January 2013 that TSA test the security effectiveness of Managed Inclusion as a system. We reported in December 2014 that according to officials, TSA anticipated that testing would begin in October 2014 and estimated that testing could take 12 to 18 months to complete.

We have also previously reported on challenges TSA has faced in designing studies and protocols to test the effectiveness of security systems and programs in accordance with established methodological practices, such as in the case of the AIT systems discussed previously

[15]GAO-15-150.

[16]See GAO-14-159; *Explosives Detection Canines: TSA Has Taken Steps to Analyze Canine Team Data and Assess the Effectiveness of Passenger Screening Canines*, GAO-14-695T (Washington, D.C.: June 24, 2014); and *Aviation Security: TSA Has Enhanced Its Explosives Detection Requirements for Checked Baggage, but Additional Screening Actions Are Needed*, GAO-11-740 (Washington, D.C.: July 11, 2011).

[17]GAO-14-159.

and in our evaluation of BDO effectiveness.[18] In our December 2014 report, we concluded that ensuring the planned effectiveness testing of the Managed Inclusion process adheres to established evaluation design practices would help TSA provide reasonable assurance that the effectiveness testing will yield reliable results.[19] In general, evaluations are most likely to be successful when key steps are addressed during design, including defining research questions appropriate to the scope of the evaluation, and selecting appropriate measures and study approaches that will permit valid conclusions. As a result, we recommended that to ensure TSA's planned testing yields reliable results, the TSA Administrator take steps to ensure that TSA's planned effectiveness testing of the Managed Inclusion process adheres to established evaluation design practices. DHS concurred with our recommendation and began taking steps toward this goal. Specifically, DHS stated that TSA plans to use a test and evaluation process—which calls for the preparation of test and evaluation framework documents including plans, analyses, and a final report describing the test results—for its planned effectiveness testing of Managed Inclusion.

[18]In November 2013, we reported on methodological weaknesses in the overall design and data collection of TSA's April 2011 validation comparison study to determine the effectiveness of the behavior detection and analysis program. For example, we found that TSA had not randomly selected airports to participate in the study, so the results were not generalizable across airports. We recommended that future funding for the program be limited until TSA provided scientifically validated evidence that demonstrates that behavioral indicators can be used to identify passengers who may pose a threat to aviation security. See GAO-14-159.

[19]GAO, *Designing Evaluations: 2012 Revision*, GAO-12-208G (Washington, D.C.: January 2012).

TSA and the FBI Have Addressed a Weakness in TSA's Oversight of Credentials for Airport Workers

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 Aviation Workers security threat assessments for airport workers.[20] Specifically, we reported 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, release dates, and probation or parole violations, among others.[21] As a result, TSA reported that its ability to look into applicant criminal history records was often incomplete.

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. TSA and the FBI have since taken steps to address this recommendation. For example, in 2014, the agencies evaluated the extent of any risk and, according to TSA and FBI officials, concluded that the risk of incomplete information did exist and could be mitigated through expanded access to state-supplied records. 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.

[20]GAO-12-60 .

[21]The FBI's criminal history records contain information from a national fingerprint and criminal history system that responds to requests from local, state, and federal agencies. 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. If an individual has a criminal record in the database, the FBI provides criminal history record check results to TSA. TSA, in turn transmits the results to the airport operator that, consistent with TSA regulations, is responsible for adjudicating the criminal history to identify potentially disqualifying criminal offenses and making a final determination of eligibility for a credential. See 49 C.F.R. § 1542.209.

Chairman Johnson, Ranking Member Carper, and members of the committee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

For questions about this statement, please contact Jennifer Grover at (202) 512-7141 or groverj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this statement include Maria Strudwick (Assistant Director), Claudia Becker, Michele Fejfar, and Tom Lombardi. Key contributors for the previous work that this testimony is based on are listed in each product.

Post-Hearing Questions for the Record
Submitted to the Honorable John Roth
From Senator Rob Portman

"Oversight of the Transportation Security Administration: First-Hand and Government Watchdog Accounts of Agency Challenges"

June 9, 2015

1. I am concerned for the safety of airline passengers given recent media reports that in an undercover investigation conducted by the Department of Homeland Security's Office of Inspector General, security screeners failed to detect weapons, mock explosives, and other prohibited items 95 percent of the time at airports across the country. How can TSA leadership work with the Office of Inspector General to address findings of the ongoing investigation and report while the report continues to be finalized?

   Response: Since the conclusion of testing on May 14, 2015, our office has had multiple briefings with TSA leadership. On June 25, 2015, our testing team met with senior officials from the Secretary's office and with TSA Assistant Administrators responsible for checkpoint screening security to discuss our testing scope, methodology, and the results of individual tests. The Secretary has assembled a working group to address the vulnerabilities identified during our testing and has invited our office to attend and observe how the Department is implementing solutions to improve checkpoint screening security.

   Additionally, on June 1, 2015, TSA shared with us its "*Proposed Action Plan to Address Preliminary Results of Inspector General Aviation Security Testing*" (Action Plan) to address the vulnerabilities we identified during testing. When we reviewed the plan, it did not include enough specificity in the actions, did not provide supporting documentation, and did not include follow-up and recurring actions to ensure the action plan will be successfully implemented and followed. However, we have been in briefings with TSA and are aware that it is developing the necessary details that may provide answers to how it intends to implement improvements. For example, on June 25, the Secretary's working group shared with us its planned presentation to the White House regarding actions TSA is taking to implement TSA's Action Plan. We look forward to reviewing TSA's future plans to address the passenger screening vulnerabilities identified during our audit.

2. The Department of Homeland Security's Office of Inspector General released a report on May 6, 2015, that found TSA does not properly manage its airport screening equipment maintenance program. TSA was found to not have issued adequate policies and procedures to airports for carrying out equipment maintenance, which can result in longer wait times, delays in passenger and baggage screening, and ultimately jeopardize passenger and aircraft safety. While TSA has concurred with the report's findings and is implementing the Office of Inspector General's recommendations, it appears that TSA regularly addresses issues only after they are identified by external Office of Inspector

General or Government Accountability Office audits. How can TSA leadership encourage a culture within TSA that is based on continuous evaluation and improvement?

Response: TSA must change from a reactive to proactive position to address emerging threats against transportation security and fulfill its mission. Although TSA made significant investments in technology and equipment to protect the Nation's transportation system, additional efforts are needed to improve its transparency and accountability. For example, in 2013 we reported that TSA's Office of Inspection's recommendations from its inspections, covert testing, and internal reviews were not always implemented. As a result, TSA may have missed opportunities to address transportation security vulnerabilities. (OIG-13-123, *Transportation Security Administration Office of Inspection's Efforts to Enhance Transportation Security*.) It is incumbent upon TSA to ensure strong management controls are in place to identify and correct vulnerabilities. TSA must also strongly encourage its personnel at all levels to identify problems and develop solutions to strengthen our aviation security system on a continuous basis.

Post-Hearing Questions for the Record
Submitted to The Honorable John Roth
From Senator Thomas R. Carper

"Oversight of the Transportation Security Administration: First-Hand and Government Watchdog Accounts of Agency Challenges"

June 9, 2015

1. We recently learned of potentially systemic failings at our Transportation Security Administration passenger screening checkpoints thanks to covert testing performed by your office. The reported rate of failure for the covert testing is simply unacceptable but, as we also learned, Secretary Johnson has already taken action to address the vulnerabilities your covert testing team exposed. Can you please provide your thoughts on Secretary Johnson's response to your office's findings regarding passenger screening as a result of covert testing?

   Response: On June 1, our covert testing team was provided with TSA's "*Proposed Action Plan to Address Preliminary Results of Inspector General Aviation Security Testing*" (Action Plan). The Action Plan encompasses a number of immediate, medium-, and long-term action items for three categories of action -- people, processes, and technology. On its face, the Action Plan represents an ambitious effort by TSA to address an array of passenger screening issues identified during both recent and prior OIG testing. This is a welcome and long overdue development.

   However, we are concerned the Action Plan (as presented) is short on details. Specifically, it lacks supporting documentation (e.g., a list of accountable parties, interim milestones/reporting requirements, and follow-up and recurring actions, etc.) needed to ensure the plan is fully-executed. The Action Plan also employs aggressive timelines which may not turn out to be realistic.

   Because the Action Plan is pre-decisional and contains classified or Sensitive Security Information, we cannot discuss or comment on the specific actions being contemplated by TSA in the public record. We would be happy to arrange a meeting with you or your staff to discuss the specific information in a closed setting.

Post-Hearing Questions for the Record
Submitted to The Honorable John Roth
From Senator Jon Tester

"Oversight of the Transportation Security Administration: First-Hand and Government Watchdog Accounts of Agency Challenges"
June 9, 2015

1. Your testimony mentions that TSA continues to fail to effectively manage its equipment and still depends too heavily on walk-through metal detectors. Did the lack of effectively deployed equipment play a role in the failures identified in the recent Red Team tests?

   Response: The audit objective of DHS OIG's covert testing team was to determine the effectiveness of TSA's Advanced Imaging Technology, Automated Target Recognition software, and checkpoint screener performance in identifying and resolving potential security threats at airport security checkpoints. The scope of this audit did not include assessing how effectively TSA has deployed equipment – including walk-thru metal detectors. As a result, we do not know the extent to which deployed equipment contributed to the passenger screening vulnerabilities identified during our current audit. Our audit involved covert testing and contains classified or Sensitive Security Information; we cannot discuss the specific results of our OIG covert testing in the public record. We would be happy to arrange a meeting with you or your staff to discuss the specific information in a closed setting. (Note: Although recent media reports widely reported on the OIG's "Red Team" results, DHS OIG's covert testing team does use this name for itself. "Red Team" is a term used by TSA's Office of Inspections for its covert testing team.)

   In fiscal year 2013, we conducted a separate audit looking at the deployment and use of Advanced Imaging Technology. (OIG-13-120 (Revised), *Transportation Security Administration's Deployment and Use of Advanced Imaging Technology.*) The objective of the audit was to determine whether TSA is effectively deploying advanced imaging technology and is fully utilizing the equipment at airports. The audit determined TSA did not develop a comprehensive deployment strategy to ensure all advanced imaging technology units were effectively deployed and fully used for screening passengers. Without a documented, approved, comprehensive plan and accurate data on the use of advanced imaging technology, TSA continued to use walkthrough metal detectors, which are unable to identify non-metallic objects. Additionally, TSA may have used resources inefficiently to purchase and deploy underused advanced imaging technology units. We issued two recommendations to TSA. TSA implemented corrective actions and both recommendations are closed.

2. Congress passed legislation last year to improve TSA's equipment management over the next five years, but do you have any thoughts on what Congress should be doing in the short-term to fix this important issue?

Response: Congress may want to consider requesting more information from TSA on its strategy for continuing to develop, implement, and maintain a robust aviation security system that is able to adapt to emerging vulnerabilities and threats based on law enforcement and intelligence data. This system should encompass not only advanced screening technologies but also employee training, internal controls, quality assurance measures and continuous monitoring to ensure TSA meets its established mission goals. To successfully strengthen and protect the Nation's transportation systems, TSA must work closely with transportation, law enforcement, and intelligence communities.

3. I remain concerned that the Screening Partnership Program (SPP) makes TSA screeners worse off and reduces moral without strong evidence that the program saves money or increases security. Can you share if any of the recent failures identified by the Red Team happened at SPP airports?

   Response: As in previous covert testing reports, our airport sample comprised airports of various sizes – including airports that participated in the Screening Partnership Program (SPP). During our most recent audit, we conducted test at two SPP airports. Generally, results were consistent across all airports. Our audit involved covert testing and contains classified or Sensitive Security Information; we cannot discuss specific results of our OIG covert testing in the public record, but would be pleased to discuss this with you or your staff in the appropriate closed setting.

4. Is your office examining TSA's security performance at SPP airports versus federal airports, or does it intend to in the near future?

   Response: While we did conduct covert tests at two SPP airports during this audit, we have not done a large-scale review of TSA's security performance at SPP airports versus federal airports that would allow us to draw across-the-board conclusions about security performance at SPP airports. We will consider adding this type of review to a future year work plan.

5. Do you think the SPP plays a role in TSA's low employee moral issues?

   Response: DHS OIG has not done any audit work in this area to date.

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

July 24, 2015

The Honorable Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs
United State Senate

Aviation Security: Responses to Posthearing Questions for the Record

Dear Mr. Chairman:

On June 9, 2015, I testified before the United States Senate Committee on Homeland Security and Governmental Affairs on the Transportation Security Administration's (TSA) Oversight of its Passenger and Airport Worker Screening Programs. This letter responds to the questions for the record that you posed. The responses are based on work associated with our previously issued products.[1] Your questions and my responses are enclosed.

If you have any questions about this letter or need additional information, please contact me at (202) 512-7141 or groverj@gao.gov

Sincerely yours,

Jennifer Grover

Jenny Grover
Director, Homeland Security and Justice Team

Enclosure

cc: cc list

[1] GAO, *Freight Rail Security: Actions Have Been Taken to Enhance Security, but the Federal Strategy Can Be Strengthened and Security Efforts Better Monitored*, GAO-09-243 (Washington D,C: April 21, 2009); *Surface Transportation Security: TSA Has Taken Actions to Manage Risk, Improve Coordination, and Measure Performance, but Additional Actions Would Enhance Its Efforts*, GAO-10-650T (Washington D,C: April 21, 2010); *Passenger Rail Security: Consistent Incident Reporting and Analysis Needed to Achieve Program Objectives*, GAO-13-20 (Washington, D.C: December 19, 2012).

1. **The overwhelming majority of attention given to Transportation Security Administration (TSA) programs relates to efforts to secure commercial aviation. However, TSA is the lead federal agency responsible for the security of all modes of transportation, including railways, highways, pipelines, and waterways. Do you believe more attention to TSA's responsibilities as it relates to surface transportation security is warranted? What specific areas of surface transportation security do you believe should receive additional attention from Congress?**

While there have been no successful terrorist attacks against the U.S. surface transportation systems to date, prior terrorist attacks on surface transportation systems in Moscow, Mumbai, London, and Madrid that caused significant loss of life and disruption have highlighted the vulnerability of transportation facilities to terrorist attacks worldwide.[2] In addition, surface transportation systems generally rely on an open architecture that is difficult to monitor and secure due to there being multiple access points, hubs serving multiple carriers, and, in some cases, a lack of access barriers. For example, America's rail network is an open system, with expanses of infrastructure spread over vast regions that often traverses densely populated urban areas. Securing surface transportation systems is also complicated by the number of private and public stakeholders involved in operating and protecting these systems, and the need to balance security with the expeditious flow of people and goods. While the Transportation Security Administration (TSA), within the Department of Homeland Security (DHS), is the primary federal agency responsible for overseeing the security of surface transportation systems, several other agencies, including DHS's Federal Emergency Management Agency (FEMA) and the Department of Transportation's (DOT) Federal Transit Administration (FTA) and Federal Railroad Administration (FRA), also play a role in helping to fund and secure these systems. In addition, unlike commercial aviation, where TSA has operational responsibility for security and performs or oversees the performance of passenger and baggage screening at most U.S. airports, TSA does not have similar responsibilities for securing surface transportation systems, but rather public and private sector transportation operators are responsible for implementing security measures for their systems. TSA's responsibilities for securing surface transportation systems have primarily included developing national strategies, establishing security standards, and conducting assessments and inspections of surface transportation modes. TSA's annual budget further highlights the difference between TSA's role in securing commercial aviation and surface transportation modes. For example, the DHS Appropriations Act, 2015, enacted March 4, 2015, appropriated $123,749,000 for surface transportation security compared to $5,639,095,000 for aviation security.[3]

Since it is not practical or feasible to protect all surface transportation assets and systems against every possible terrorist threat, DHS has called for using risk-informed approaches to prioritize its security-related investments and for developing plans and allocating resources in a way that balances security and commerce. While DHS has taken actions to implement a risk management approach to securing surface transportation systems we have previously reported

[2] Subway attacks occurred in Moscow on March 29, 2010, Mumbai on July 11, 2006, London on July 7, 2005, and Madrid on March 11, 2004. Each attack caused dozens of deaths and injuries.

[3] Pub. L. No. 114-4, 129 Stat. 39, 44-46 (2015). The approximately $124 million and $5.6 billion appropriated to TSA's "Surface Transportation Security" and "Aviation Security" accounts, respectively, does not reflect amounts appropriated to TSA's "Intelligence and Vetting" and "Transportation Security Support" accounts, which also support TSA's surface and aviation security missions, as well as the $250 million in fee collections available to TSA through the Aviation Security Capital Fund to support security-related airport improvement projects and the procurement and installation of explosives detection systems for use at airports.

that it could do more to inform resource allocation based on risk across the surface transportation sector—including the mass transit and passenger rail, freight rail, highway, and pipeline modes. Moreover, our prior work in this area highlights the importance of (1) comprehensive risk assessment to guide investment decisions, (2) coordination with stakeholders and across federal agencies, and (3) coordinated oversight of security requirements and reporting of incidents to allow identification of trends. These are issues of enduring importance that continue to be worthy of Congressional attention. We have provided additional information below on each of these areas.

In March 2009, GAO reported that TSA had not conducted comprehensive risk assessments to compare risk across the entire transportation sector, which the agency could use to guide investment decisions, and recommended that TSA do so. In June 2010, TSA produced the Transportation Sector Security Risk Assessment (TSSRA), which assessed risk within and across the aviation, mass transit, highway, freight rail, and pipeline modes, and incorporated threat, vulnerability, and consequence.

In addition, we reported in April 2009 that while TSA has generally improved coordination with key surface transportation stakeholders, additional actions could enhance its efforts, such as sharing relevant freight rail threat assessment information to avoid duplication of effort, among other things. TSA has since taken several steps to better ensure federal agencies coordinate as effectively as possible, including ensuring relevant freight rail assessments and information are shared and that TSA and FRA field inspector resources are better leveraged. Specifically, TSA, prior to assessing a railroad bridge, now obtains any prior DHS Infrastructure Protection (IP) assessments of the same bridge in order to fully leverage relevant information and analysis before conducting their own assessment. In addition, in 2012, TSA and DHS IP signed an Information Sharing and Access Agreement (ISAA) to define the roles and responsibilities of IP and TSA in collaboratively sharing specific transportation sector-related risk information.

More recently, in December 2012, GAO reported that TSA was not consistently providing consistent oversight for its rail security incident reporting requirement because of, among other things, a lack of guidance leading to considerable variation in the types and number of incidents reported. For example, local TSA officials instructed one rail agency to report all incidents related to individuals struck by trains, while local TSA officials for another rail agency said these incidents would not need to be reported as they are most often suicides with no nexus to terrorism. GAO also found inconsistency in TSA compliance inspections and enforcement actions because, among other things, TSA's rail security inspection policies did not specify inspection frequency, but rather called for performing a "reasonable number" of inspections. For example, 3 of the 19 rail agencies GAO contacted were not inspected from January 2011 through June 2012, including a large metropolitan rail agency. In addition, TSA took enforcement action against an agency for not reporting an incident involving a knife, but did not take action against another agency for not reporting similar incidents, though the agency had been inspected. As a result, GAO recommended that TSA develop guidance on the types of incidents that should be reported, and enhance existing oversight mechanisms for compliance inspections and enforcement actions. TSA concurred with our recommendations and has since taken action to address these deficiencies. Specifically, in September 2013, TSA disseminated written guidance to local TSA inspection officials and rail agencies that provided clarification about the requirements of the rail security incident reporting process, and included examples and descriptions of the types of incidents that should be reported under the regulatory criteria, as well as details about the type of information that should be included in the incident report provided to the Transportation Security Operations Center. In addition, TSA provided Surface Regional Security Inspectors (RSI) with the ability to review both passenger and freight rail

inspections in the Performance and Results Information System (PARIS) before the inspections are finalized and any enforcement actions are taken. TSA also established an RSI-dashboard report that provides weekly, monthly, and quarterly information about the number of inspections that have been reviewed, accepted, and rejected, and developed a mechanism for tracking the recommendations RSIs make to local TSA inspection officials regarding changes to local compliance inspections, as well as any actions that are taken in response. This mechanism allows the RSIs to provide management oversight of passenger and freight rail regulatory inspections and enforcement actions, which helps ensure that these regulations are consistently implemented and enforced.