

REFORM AND IMPROVEMENT: ASSESSING THE  
PATH FORWARD FOR THE TRANSPORTATION  
SECURITY ADMINISTRATION

---

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

OCTOBER 8, 2015

**Serial No. 114-36**

Printed for the use of the Committee on Homeland Security



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

U.S. GOVERNMENT PUBLISHING OFFICE

99-578 PDF

WASHINGTON : 2016

---

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

## COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

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

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

---

## SUBCOMMITTEE ON TRANSPORTATION SECURITY

JOHN KATKO, New York, *Chairman*

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

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

# CONTENTS

	Page
STATEMENTS	
The Honorable John Katko, a Representative in Congress From the State of New York, and Chairman, Subcommittee on Transportation Security .....	1
The Honorable Kathleen M. Rice, a Representative in Congress From the State of New York, and Ranking Member, Subcommittee on Transportation Security:	
Oral Statement .....	3
Prepared Statement .....	4
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:	
Oral Statement .....	4
Prepared Statement .....	5
WITNESSES	
Honorable John Roth, Inspector General, Office of Inspector General, U.S. Department of Homeland Security:	
Oral Statement .....	6
Prepared Statement .....	8
Honorable Peter Neffenger, Administrator, Transportation Security Administration, U.S. Department of Homeland Security:	
Oral Statement .....	24
Prepared Statement .....	26
FOR THE RECORD	
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:	
List .....	39
APPENDIX	
Questions From Chairman John Katko for Peter Neffenger .....	45
Questions From Ranking Member Bennie G. Thompson for Peter Neffenger ...	50
Questions From Honorable William R. Keating for Peter Neffenger .....	52
Questions From Chairman John Katko for John Roth .....	53



## **REFORM AND IMPROVEMENT: ASSESSING THE PATH FORWARD FOR THE TRANSPORTATION SECURITY ADMINISTRATION**

**Thursday, October 8, 2015**

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

The subcommittee met, pursuant to call, at 3:13 p.m., in Room 311, Cannon House Office Building, Hon. John Katko [Chairman of the subcommittee] presiding.

Present: Representatives Katko, Carter, Rice, Keating, and Thompson.

Mr. KATKO. The Committee on Homeland Security Subcommittee on Transportation Security will come to order. The subcommittee is meeting today to hear testimony on assessing the future of the Transportation Security Administration. I now recognize myself for an opening statement.

I would like to welcome everyone to today's hearing and I am pleased to have Inspector General Roth back once again and Administrator Neffenger again back here as well. The purpose of today's hearing is to examine TSA's challenges and identify what changes TSA needs to make in order to move forward in an effective manner.

TSA was created out of a tragedy and was quickly stood up to address major security vulnerabilities that terrorists exploited. However, 14 years after 9/11, we now have an agency that has had many missteps in its efforts to keep the traveling public safe.

Inspector General Roth, your office has conducted over 100 audits identifying major security vulnerabilities and organizational challenges throughout TSA, including the most recent reports that found that TSA passenger screening was allegedly wrong 96 percent of the time. And that 73 aviation workers had potential ties to terrorism. Of course, there is also the recent cases involving drug trafficking incidents in airports at Dallas/Fort Worth, Los Angeles International, and Oakland, to name a few involving employees. These figures are startling and shatter the public confidence.

I look forward to hearing from you today about what systemic problems you have identified and what needs to be done to help TSA address these challenges.

What is most unfortunate is that these startling findings by both your office, and the Government Accountability Office, as well as the FBI and other agencies, are not isolated instances. Many of

these vulnerabilities have been identified and known for years, and unfortunately, prior to this year the previous leadership in both TSA and DHS did not take the appropriate steps to address these known security vulnerabilities. The purpose of today's hearing is not to look backwards, however.

With new leadership, Administrator Neffenger, you have an opportunity to address these challenges head on, and lead TSA in a different path, and I am confident that you will do so. In our discussions you have been frank, straightforward, and sincere and I appreciate that. I have full confidence that you are tackling TSA's challenges with an open mind. I look forward to hearing from you today about how we can work together to ensure TSA fulfills its critical mission.

This subcommittee has worked tirelessly and in an overwhelmingly bipartisan manner to address the challenges that TSA faces. Since the start of this Congress we have had 7 pieces of legislation pass the House, which is remarkable out of this committee, and 2 of those bills are now public laws. However, there is no silver bullet to address all of the challenges that TSA faces, and unfortunately, we have to be right 100 percent of the time and the terrorists have to be right just once.

With nearly 2 million passengers being screened every day we need to do more to better focus our efforts on those passengers that are unknown while still taking precautions to protect against the insider threat.

Currently, less than 5 percent of travellers participate in PreCheck. TSA needs to increase this population so that it can target its efforts and resources in a more risk-based manner. That is why I introduced H.R. 2843, the PreCheck Expansion Act. This bill will help TSA to take steps to effectively and robustly market the program and dramatically increase the enrollment. However, in addition to expanding PreCheck, TSA must look at what additional efforts are necessary to increase the security effectiveness of PreCheck and what measures are necessary to mitigate the insider threat.

This week the House passed H.R. 3102, the Airport Access Control Security Improvement Act of 2015. This legislation which I introduced earlier this year requires TSA to consult with Federal and private-sector partners to review existing employee screening protocols and work in a comprehensive manner to improve the effectiveness of access controls at airports across the United States. It is a major undertaking.

We must do a better job at knowing more about the people who work and travel through our Nation's airports. Securing our Nation's transportation systems is of vital importance to both our National security, and our economic strength, and stability.

In the 9/11 Commission report, the then head of the CIA, George Tenet was quoted as saying, "The system was blinking red," in the months leading up to 9/11. We cannot stand idly by and grant tacit approval to lax security measures when we have the authority, responsibility, and indeed the duty to spur action and keep the traveling public safe from harm.

Inspector General Roth, Administrator Neffenger, this committee wants to support both of you in your efforts to reform TSA. We look

forward to hearing from you today. You are not on opposite sides of the fence. I view you both on the same side of the fence: One exposing the problems, the other one making sure they get fixed. That is why you are both here today.

With that, I recognize the Ranking Member of the subcommittee, the gentlelady from New York, Miss Rice for an opening statement.

Miss RICE. Thank you, Mr. Chairman, and thank you for convening this hearing. I would also like to thank the witnesses for being here today to discuss the need for and status of reforms and improvements within the TSA.

Administrator Neffenger, I understand you had to adjust your schedule in order to testify before this subcommittee today and I want to tell you how much we appreciate that. While you have only been in this position since June, you have demonstrate a true commitment to work constructively with us as you take on the challenges facing TSA and I thank you for that.

Finally, I want to thank Inspector General Roth for being here today and for the work you have done and continue to do, to identify vulnerabilities within TSA and advise us on what we can do to enhance the security of our commercial aviation sector. Your most recent report which is Classified, concerns covert tests conducted by undercover DHS investigators who attempted to smuggle prohibited items, including weapons and mock explosives past TSA security checkpoints. As we all know the results of these covert tests were leaked to the media in June before the report was complete, and it was reported that in 67 out of 70 tests, TSA failed to detect these items and allowed the investigators to proceed past the checkpoint.

Sixty-seven out of 70, that is 96 percent of the time. I think we can all agree that 96 percent is an alarming figure, and one that we cannot overlook. We have to assess all of the findings and recommendations in your report. We have to shine a light on the vulnerabilities that these covert tests have exposed, and we have to take action to eliminate those vulnerabilities.

We know that the threats to this country, particularly to our aviation sector, are constant. They are real. We know those threats are evolving and becoming more sophisticated, but the people who want to do us harm are always on the watch for a new way in, a new way to beat the system. That is why we have to be even more vigilant. That is why we conduct these tests. Because we know that no matter how good our security might be, it can be better. It can always be better and the findings in this report make it clear that it can and must be much better in order to match the threats that we face today.

So I am eager to hear how our witnesses are working together to act on these findings, to implement reforms, and to close the gaps that these covert tests uncovered.

Obviously, as we all know, Administrator Neffenger, you have only been in your position for a few months. Many of the topics and reports that Inspector General Roth has compiled pre-date your time at TSA, but I certainly look forward to hearing what TSA is doing in response to this most recent report, and if Inspector General Roth has previously identified other security gaps or

vulnerabilities that TSA must still address, I would like to learn about those efforts as well.

Mr. Chairman, thank you again for convening this hearing. I look forward to productive dialogue today. I yield back the balance of my time.

[The statement of Miss Rice follows:]

STATEMENT OF RANKING MEMBER KATHLEEN RICE

OCTOBER 8, 2015

Administrator Neffenger, while you've only been in this position since June, you've demonstrated a real commitment to work constructively with us as you take on the challenges facing TSA, and I thank you for that.

Finally, I want to thank Inspector General Roth for being here today and for the work you have done and continue to do to identify vulnerabilities within TSA and advise us on what we can do to enhance the security of our commercial aviation sector.

Your most recent report, which is Classified, concerns covert tests conducted by undercover DHS investigators who attempted to smuggle prohibited items—including weapons and mock explosives—past TSA airport security checkpoints.

As we all know, the results of these covert tests were leaked to the media in June, before the report was complete, and it was reported that in 67 out of 70 tests, TSA failed to detect these items and allowed the investigators to proceed past the checkpoint. Sixty-seven out of 70—that's 96 percent.

I think we can all agree that 96 percent is an alarming figure, and one that we cannot overlook.

We have to assess all of the findings and recommendations in your report, we have to shine a light on the vulnerabilities that these covert tests have exposed, and we have to take action to eliminate those vulnerabilities.

We know that the threats to this country, particularly to our aviation sector, are constant. We know those threats are evolving and becoming more sophisticated, that the people who want to do us harm are always on the watch for a new way in, a new way to beat the system.

That's why we have to be even more vigilant, that's why we conduct these tests—because we know that no matter how good our security might be, it can be better. It can always be better—and the findings in this report make it clear that it can and must be much better in order to match the threats we face today.

So I'm eager to hear how our witnesses are working together to act on these findings, implement reforms, and close the gaps that these covert tests uncovered.

I know that Administrator Neffenger has been in his position for only a few months, and that many of the topics and reports that Inspector General Roth has compiled pre-date the administrator's time at TSA.

But I certainly look forward to hearing what TSA is doing in response to this most recent report. And if Inspector General Roth has previously identified other security gaps or vulnerabilities that TSA must still address, I would like to learn about those efforts as well.

Mr. KATKO. Thank you, Miss Rice.

The Chair now recognizes the Ranking Minority Member of the full committee, the gentleman from Mississippi, Mr. Thompson, for any statement he may have.

Mr. THOMPSON. Thank you very much, Chairman Katko and Ranking Member Rice, for holding today's hearing. Also, I welcome the administrator and the Inspector General for their appearance also.

Throughout this Congress, this committee has voiced its concern with the state of security within the commercial aviation sector. Over the span of recent years, both Inspector General and the Government Accountability Office, have compiled numerous reports that detail mismanagement, inefficiencies, and vulnerabilities within TSA. These reports range from vulnerabilities associated with granting expedited screening via the use of Secure Flight and Man-



aged Inclusion, to vulnerabilities associated with access to secure areas of airports, and the tracking of maintenance for security-related technologies within airports.

Most recently, the Inspector General released a report *Covert Testing of TSA's Passenger Screening Technologies and Processes at Airport Security Checkpoints*. Details of this Classified report were leaked this summer and the Inspector General has given a briefing on the final report to this subcommittee. While I look forward to hearing the status of solutions that TSA and DHS are implementing to ensure that any security gaps associated with checkpoint screening and technologies are secure, our main concern is that TSA will continue to purchase more technologies that address the threats of yesterday instead of the threats of tomorrow.

Consequently, the Transportation Security Administration Reform and Improvement Act of 2015, a bill that recently passed the committee, includes language that aims to aid in the development and innovative security technologies through a program that would create public and private-sector partnerships to help businesses, particularly small businesses, to commercialize these innovative technologies. While that amendment is designed to improve the technologies TSA uses, I still have concerns about some of TSA's other screening programs the Inspector General has found ineffective.

For example, the Inspector General has found that TSA's behavioral detection program commonly referred to as SPOT is a magnet for racial profiling, and TSA has little evidence that the program is an effective tool for screening passengers. We know that terrorists span all races, in all ethnicities, and have a profiling mechanism as a means of security is skeptical. Once again, I ask the administrator to review its efficiency of the behavioral detection program.

While the administrator appeared before the committee on July 1, I, along with many of my colleagues across the aisle, stated that we would give him appropriate time to address some of these glaring concerns at TSA. So Mr. Administrator, we are glad to have you. I would assume the honeymoon is about over, and we can move forward. So I look forward to your testimony and I yield back.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

OCTOBER 8, 2015

Throughout this Congress, this committee has voiced its concerns with the state of security within the commercial aviation sector. Over the span of recent years, both the Inspector General and the Government Accountability Office have compiled numerous reports that detail mismanagement, inefficiencies, and vulnerabilities within TSA.

These reports range from vulnerabilities associated with granting expedited screening via the use of Secure Flight and Managed Inclusion, to vulnerabilities associated with access to the secure areas of airports and the tracking of maintenance for security-related technologies within airports.

Most recently, the Inspector General released a report, "*Covert Testing of TSA's Passenger Screening Technologies and Processes at Airport Security Checkpoints*." Details of this Classified report were leaked this summer, and the Inspector General has given a briefing on the final report to the subcommittee.

While I look forward to hearing the status of solutions that TSA and DHS are implementing to ensure that any security gaps associated with checkpoint screening and technologies are secure, I remain concerned that TSA will continue to purchase

more technologies that address the threats of yesterday instead of the threats of tomorrow.

Consequently, the “Transportation Security Administration Reform and Improvement Act of 2015” a bill that recently passed the committee includes language that aims to aid in the development of innovative security technologies through a program that would create public and private-sector partnerships to help businesses, particularly small businesses, to commercialize these innovative technologies.

And while that amendment is designed to improve the technologies TSA uses, I still have concerns about some of TSAs other screening programs the Inspector General has found ineffective. For example, the Inspector General has found that TSA’s behavioral detection program, commonly known as SPOT, is a magnet for racial profiling and TSA has little evidence that the program is an effective tool for screening passengers.

We know that terrorists span all races and ethnicities and having a profiling mechanism as a means of security is skeptical. Once again, I ask the administrator to review its efficacy of behavioral detection programs.

When the administrator appeared before the committee in July, I, along with my colleagues across the aisle, stated that we would give him appropriate time to address some of the glaring concerns at TSA. It is unrealistic to expect sweeping reforms to have been made in such a short amount of time, and I want to express my appreciation for the administrator’s agreeing with Congress that the Managed Inclusion program was flawed and needed to be phased out.

Even though the Inspector General’s reports have been scathing, I am optimistic that the culture of TSA and the willingness to take the recommendations from these reports and implement reforms is improving.

I am interested in hearing how these entities work together to take the issues found within these investigations and audits and use them to create solutions that will keep the traveling public safe.

Mr. KATKO. Thank you, Mr. Chairman. Other Members of the committee are reminded that opening statements may be submitted for the record.

We are pleased to have a group of distinguished witnesses before us today, as I mentioned, to speak on this important topic, and are no strangers to this subcommittee. Let me remind the witnesses that their entire written statements will appear in the record.

Our first witness is The Honorable John Roth, who currently serves as Inspector General of the Department of Homeland Security. Prior to his appointment as Inspector General, Mr. Roth served as the director of the Office of Criminal Investigations at the Food and Drug Administration, was chief of staff to the Deputy Attorney General and worked at the Narcotic and Dangerous Drugs Section, which is the best section in all of the Department of Justice. Am I right?

Mr. ROTH. You are close, yes.

Mr. KATKO. Because we both worked there. The Chair now recognizes Mr. Roth to testify.

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

Mr. ROTH. Good afternoon, Chairman Katko, Ranking Member Rice, and Members of the subcommittee. Thank you for inviting me here to testify today.

Throughout this year I have testified before this subcommittee and others regarding TSA’s ability to execute its important mission. I highlighted the challenges that TSA faced. I testified that these challenges were in almost every area of TSA’s operations. Its problematic implementation of risk assessment rules, including its management of TSA PreCheck, failures in passenger and baggage

screen operations, TSA's control over access to secure areas including management of its access badge program, its management of the Workforce Integrity program, its oversight over acquisition and maintenance of screening equipment, and other issues that we have discovered in the course of over 115 audits and inspection reports.

These issues were exacerbated, in my judgment, by a culture that developed over time which resisted oversight and was unwilling to accept the need for change in the face of an evolving and serious threat. We have been writing reports highlighting some of these problems for years without an acknowledgment by TSA of the need to correct its deficiencies. However, we may be in a very different place now than we were then. I am hopeful that Administrator Neffenger brings with him a new attitude about oversight. Ensuring transportation safety is a massive and complex problem and there is no single silver bullet to solve it. It will take a sustained and disciplined effort.

The first step, however, in fixing this problem is having the courage to critically assess the deficiencies in an honest and objective light, creating a culture of change within TSA, and giving the TSA workforce the ability to identify and address risks will be the administrator's most critical and challenging task. I believe that the Department and TSA leadership has begun that process of critical self-evaluation and aided by the workforce at TSA are in a position to address some of these issues. As you noted, we have just completed and distributed a report on our most recent round of covert testing of TSA's checkpoint operations. The results, while Classified, were disappointing.

Our testing was designed to check test point operations in real-world conditions. The failures included failures in technology, failures in TSA procedures, and human error. We found layers of security simply missing. But these results were not unexpected. We had conducted other covert testing in the past with similar results.

TSA has put forward a plan consistent with our recommendation to improve checkpoint quality in three areas: Technology, personnel, and procedures. This plan is appropriate because the checkpoint must be considered as a single system. The most effective technology is useless without the right personnel, and the personnel need to be guided by the appropriate procedures. Unless all three elements are operating efficiently, the checkpoint will not be effective.

We will be monitoring TSA's efforts to increase the effectiveness of checkpoint operations and will continue to conduct covert testing. Consistent with our obligations under the Inspector General Act, we will report our results to this committee, as well as other committees of jurisdiction.

While this audit focused on the checkpoint, effective checkpoint operations in and of themselves are not enough. We must also look at other areas to determine vulnerabilities. We have done considerable work on TSA's assessment of passenger risk, and have registered our concern about TSA's use of Managed Inclusion and risk rules that were not based on an individual assessment of passenger risk. I am pleased to report that TSA has phased out its use of Managed Inclusion. However, we still have outstanding rec-

ommendations regarding the risk assessment rules that TSA continues to use. I urge the administrator to consider whether or not those risk rules are effective and ensure the safety of the transportation public.

TSA also has the responsibility to oversee and regulate airport security provided by airport authorities. For example, in the case of airport worker vetting, TSA relies on airports to submit a complete and accurate aviation worker application data for vetting. In a recent audit we found that TSA does not ensure that airports have a robust verification process for criminal history, and authorization to work in the United States, or sufficiently track the results of their review. TSA also did not have an adequate monitoring process in place to ensure that airport operators properly adjudicated applicants' criminal histories.

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

[The prepared statement of Mr. Roth follows:]

PREPARED STATEMENT OF JOHN ROTH

OCTOBER 8, 2015

Good afternoon Chairman Katko, Ranking Member Rice, and Members of the subcommittee.

Thank you for inviting me here today to discuss our work on the Transportation Security Administration (TSA). Our reviews have given us a perspective on the obstacles facing TSA in carrying out an important—but incredibly difficult—mission to protect the Nation's transportation systems and ensure freedom of movement for people and commerce.

Throughout this year, I have testified—before this subcommittee and others—regarding my concerns about TSA's ability to execute its important mission. I highlighted the challenges TSA faced. I testified that these challenges were in almost every area of TSA's operations: Its problematic implementation of risk assessment rules, including its management of TSA PreCheck; failures in passenger and baggage screening operations, discovered in part through our covert testing program; TSA's controls over access to secure areas, including management of its access badge program; its management of the workforce integrity program; TSA's oversight over its acquisition and maintenance of screening equipment; and other issues we have discovered in the course of over 115 audit and inspection reports.

My remarks were described as “unusually blunt testimony from a Government witness,” and I will confess that it was. However, those remarks were born of frustration that TSA was assessing risk inappropriately and did not have the ability to perform basic management functions in order to meet the mission the American people expect of it. These issues were exacerbated, in my judgment, by a culture, developed over time, which resisted oversight and was unwilling to accept the need for change in the face of an evolving and serious threat. We have been writing reports highlighting some of these problems for years without an acknowledgment by TSA of the need to correct its deficiencies.

We may be in a very different place than we were in May. I am hopeful that Administrator Neffenger brings with him a new attitude about oversight. Ensuring transportation safety is a massive and complex problem, and there is no silver bullet to solve it. It will take a sustained and disciplined effort. However, the first step in fixing a problem is having the courage to critically assess the deficiencies in an honest and objective light. Creating a culture of change within TSA, and giving the TSA workforce the ability to identify and address risks without fear of retribution, will be the new administrator's most critical and challenging task.

I believe that the Department and TSA leadership have begun the process of critical self-evaluation and, aided by the dedicated workforce of TSA, are in a position to begin addressing some of these issues. I am hopeful that the days of TSA sweeping its problems under the rug and simply ignoring the findings and recommendations of the OIG and GAO are coming to an end.

I have been gratified by the Department's response and believe that this episode serves as an illustration of the value of the Office of Inspector General, particularly

when coupled with a Department leadership that understands and appreciates objective and independent oversight.

#### OUR MOST RECENT COVERT TESTING

We have just completed and distributed our report on our most recent round of covert testing. The results are classified at the Secret level, and the Department and this committee have been provided a copy of our Classified report. TSA justifiably classifies at the Secret level the validated test results; any analysis, trends, or comparison of the results of our testing; and specific vulnerabilities uncovered during testing. Additionally, TSA considers other information protected from disclosure as Sensitive Security Information.

While I cannot talk about the specifics in this setting, I am able to say that we conducted the audit with sufficient rigor to satisfy the standards contained within the Generally Accepted Government Auditing Standards, that the tests were conducted by auditors within our Office of Audits without any special knowledge or training, and that the test results were disappointing and troubling. We ran multiple tests at 8 different airports of different sizes, including large Category X airports across the country, and tested airports using private screeners as part of the Screening Partnership Program. The results were consistent across every airport.

Our testing was designed to test checkpoint operations in real-world conditions. It was not designed to test specific, discrete segments of checkpoint operations, but rather the system as a whole. The failures included failures in the technology, failures in TSA procedures, and human error. We found layers of security simply missing. It would be misleading to minimize the rigor of our testing, or to imply that our testing was not an accurate reflection of the effectiveness of the totality of aviation security.

The results were not, however, unexpected. We had conducted other covert testing in the past:

- In September 2014, we conducted covert testing of the checked baggage screening system and identified significant vulnerabilities in this area caused by human and technology based failures. We also determined that TSA did not have a process in place to assess or identify the cause for equipment-based test failures or the capability to independently assess whether deployed explosive detection systems are operating at the correct detection standards. We found that, notwithstanding an intervening investment of over \$550 million, TSA had not improved checked baggage screening since our 2009 report on the same issue. (*Vulnerabilities Exist in TSA's Checked Baggage Screening Operations*, OIG-14-142, Sept. 2014)
- In January 2012, we conducted covert testing of access controls to secure airport areas and identified significant access control vulnerabilities, meaning uncleared individuals could have unrestricted and unaccompanied access to the most vulnerable parts of the airport—the aircraft and checked baggage. (*Covert Testing of Access Controls to Secured Airport Areas*, OIG-12-26, Jan. 2012)
- In 2011, we conducted covert penetration testing on the previous generation of AIT machines in use at the time; the testing was far broader than the most recent testing, and likewise discovered significant vulnerabilities. (*Penetration Testing of Advanced Imaging Technology*, OIG-12-06, Nov. 2011)

#### THE DHS RESPONSE

The Department's response to our most recent findings has been swift and definite. For example, within 24 hours of receiving preliminary results of OIG covert penetration testing, the Secretary summoned senior TSA leadership and directed that an immediate plan of action be created to correct deficiencies uncovered by our testing. Moreover, DHS has initiated a program—led by members of Secretary Johnson's leadership team—to conduct a focused analysis on issues that the OIG has uncovered, as well as other matters. These efforts have already resulted in significant changes to TSA leadership, operations, training, and policy, although the specifics of most of those changes cannot be discussed in an open setting, and should, in any event, come from TSA itself.

TSA has put forward a plan, consistent with our recommendations, to improve checkpoint quality in three areas: Technology, personnel, and procedures. This plan is appropriate because the checkpoint must be considered as a single system: The most effective technology is useless without the right personnel, and the personnel need to be guided by the appropriate procedures. Unless all three elements are operating effectively, the checkpoint will not be effective.

We will be monitoring TSA's efforts to increase the effectiveness of checkpoint operations and will continue to conduct covert testing. Consistent with our obligations

under the Inspector General Act, we will report our results to this subcommittee as well as other committees of jurisdiction.

We have also been making significant progress on many outstanding recommendations from prior reports.

#### TSA AND THE ASYMMETRIC THREAT

Nowhere is the asymmetric threat of terrorism more evident than in the area of aviation security. TSA cannot afford to miss a single, genuine threat without potentially catastrophic consequences, and yet a terrorist only needs to get it right once. Securing the civil aviation transportation system remains a formidable task—TSA is responsible for screening travelers and baggage for over 1.8 million passengers a day at 450 of our Nation's airports. Complicating this responsibility is the constantly-evolving threat by adversaries willing to use any means at their disposal to incite terror.

The dangers TSA must contend with are complex and not within its control. Recent media reports have indicated that some in the U.S. intelligence community warn terrorist groups like the Islamic State (ISIS) may be working to build the capability to carry out mass casualty attacks, a significant departure from—and posing a different type of threat—than simply encouraging lone-wolf attacks. According to these media reports, a mass casualty attack has become more likely in part because of a fierce competition with other terrorist networks: Being able to kill opponents on a large scale would allow terrorist groups such as ISIS to make a powerful showing. We believe such an act of terrorism would likely be designed to impact areas where people are concentrated and vulnerable, such as the Nation's commercial aviation system.

#### MERE INTELLIGENCE IS NOT ENOUGH

In the past, officials from TSA, in testimony to Congress, in speeches to think tanks, and elsewhere, have described TSA as an intelligence-driven organization. According to TSA, it continually assesses intelligence to develop countermeasures in order to enhance these multiple layers of security at airports and on-board aircraft. This is a necessary thing, but it is not sufficient.

In the vast majority of the instances, the identities of those who commit terrorist acts were simply unknown to or misjudged by the intelligence community. Terrorism, especially suicide terrorism, depends on a cadre of newly-converted individuals who are often unknown to the intelligence community. Moreover, the threat of ISIS or al-Qaeda-inspired actors—those who have no formal ties to the larger organizations but who simply take inspiration from them—increases the possibilities of a terrorist actor being unknown to the intelligence community.

Recent history bears this out:

- 17 of the 19 September 11 hijackers were unknown to the intelligence community. In fact, many were recruited specifically because they were unknown to the intelligence community.
- Richard Reid, the 2002 “shoe bomber,” was briefly questioned by the French police, but allowed to board an airplane to Miami. He had the high explosive PETN in his shoes, and but for the intervention of passengers and flight crew, risked bringing down the aircraft.
- The Christmas day 2009 bomber, who was equipped with a sophisticated non-metallic explosive device provided by al-Qaeda, was known to certain elements of the intelligence community but was not placed in the Terrorist Screening Database, on the Selectee List, or on the No-Fly List. A bipartisan Senate report found there were systemic failures across the intelligence community, which contributed to the failure to identify the threat posed by this individual.
- The single most high-profile domestic terrorist attack since 9/11, the Boston Marathon bombing, was masterminded and carried out by Tamerlan Tsarnaev, an individual who approximately 2 years earlier was judged by the FBI not to pose a terrorist threat, and who was not within any active U.S. Government databases.

Of course, there are instances in which intelligence can foil plots that screening cannot detect—such as the 2006 transatlantic aircraft plot, utilizing liquid explosives; the October 2010 discovery of U.S.-bound bombs concealed in printer cartridges on cargo planes in England and Dubai; and the 2012 discovery that a second generation nonmetallic device, designed for use on-board aircraft, had been produced.

What this means is that there is no easy substitute for the checkpoint. The checkpoint must necessarily be intelligence-driven, but the nature of terrorism today means that each and every passenger must be screened in some way.

## BEYOND THE CHECKPOINT

Much of the attention has been focused on the checkpoint, since that is the primary and most visible means of entry onto aircraft. But effective checkpoint operations simply are not of themselves sufficient. Aviation security must also look at other areas to determine vulnerabilities.

*Assessment of passenger risk*

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 had deep concerns about some of TSA's previous 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. Starting in 2012, TSA massively increased the use of PreCheck. Some of the expansion, for example allowing PreCheck to other Federal Government-vetted or known flying populations, such as those in the CBP Trusted Traveler Program, made sense. In addition, TSA continues to promote participation in PreCheck by passengers who apply, pay a fee, and undergo individualized security threat assessment vetting. I am encouraged by legislation, originating in this subcommittee, H.R. 2843, the *TSA PreCheck Expansion Act*, which I believe would further improve the use of PreCheck operations.

However, we believe that TSA's use of risk assessment rules, which granted expedited screening to broad categories of individuals unrelated to an individual assessment of risk, but rather on some questionable assumptions about relative risk based on other factors, created an unacceptable risk to aviation security.<sup>1</sup> Additionally, TSA used "managed inclusion" for the general public, allowing random passengers access to PreCheck lanes with no assessment of risk. Additional layers of security TSA intended to provide, which were meant to compensate for the lack of risk assessment, were often simply not present.

We made a number of recommendations as a result of several audits and inspections. Disappointingly, when the report was issued, TSA did not concur with the majority of our 17 recommendations. At the time, I testified that I believed this represented TSA's failure to understand the gravity of the risk that they were assuming. I am pleased to report, however, that we have recently made significant progress in getting concurrence and compliance with these recommendations.

For example, I am pleased to report that TSA's practice of using Managed Inclusion has been eliminated. As you know, this subcommittee held a hearing on the issue of expedited screening in March, at which I expressed my significant concerns. TSA disagreed with that finding notwithstanding our recommendation and continued to use Managed Inclusion. Now, however, I am pleased to report that TSA has reversed its decision.

However, that report still has an outstanding recommendation regarding the risk assessment rules to grant expedited screening through PreCheck lanes. Unfortunately, TSA continues to use these risk rules.

There is pending legislation originating in this subcommittee, H.R. 3584—the *Transportation Security Administration Reform and Improvement Act of 2015*, which has been introduced—that would eliminate the practice. I urge the administrator to reconsider, in advance of the passage of this legislation, TSA's non-concurrence with our recommendation and stop the practice.

*Access to secure areas*

TSA is responsible, in conjunction with the 450 airports across the country, to ensure that the secure areas of airports, including the ability to access aircraft and checked baggage, are truly secure. In our audit work, we have had reason to question whether that has been the case. We conducted covert testing in 2012 to see if auditors could get access to secure areas by a variety of means. While the results of those tests are Classified, they were similar to the other covert testing we have done, which was disappointing.

Additionally, as we discuss below, TSA's oversight of airports when it comes to employee screening needs to be improved. (*TSA Can Improve Aviation Worker Vetting (Redacted)*, OIG-15-98, June 2015)

I have reviewed the work of this subcommittee as well, and am aware of the significant vulnerabilities that have been uncovered in the course of criminal investigations and this subcommittee's hearings. We are encouraged by the introduction of

<sup>1</sup>As an example of PreCheck's vulnerabilities, we reported that, through risk assessment rules, a felon who had been imprisoned for multiple convictions for violent felonies while participating in a domestic terrorist group was granted expedited screening through PreCheck.

H.R. 3102, the *Airport Access Control Security Improvement Act of 2015*, which requires TSA to establish a risk-based screening model for airport employees, to look at the current list of disqualifying offenses, to improve the auditing procedures TSA uses to check on airport badging operations, and to make other improvements.

We are doing additional audit and inspection work in this area, determining whether controls over access media badges issued by airport operators is adequate. We are also engaging in an audit of the screening process for the Transportation Worker Identification Credential program (TWIC) to see whether it is operating effectively and whether the program's continued eligibility processes ensures that only eligible TWIC card holders remain eligible.

*Other questionable investments in aviation security*

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 fiscal years 2007 through 2012.

We understand the desire to have such a program. Israel is foremost in their use of non-physical screening, although the differences in size, culture, and attitudes about civil liberties make such a program difficult to adopt in this country. In the United States, sharp-eyed Government officials were able to assess behavior to prevent entry to terrorists on two separate occasions:

- Ahmed Ressam's plot to blow up the Los Angeles International Airport on New Year's Eve 1999 was foiled when a U.S. Customs officer in Port Angeles, Washington, thought Ressam was acting "hinky" and directed a search of his car, finding numerous explosives and timers.
- In 2001, a U.S. immigration officer denied entry to the United States to Mohammed al Qahtani, based on Qahtani's evasive answers to his questions. Later investigation by the 9/11 Commission revealed that Qahtani was to be the 20th hijacker, assigned to the aircraft that ultimately crashed in Shanksville, Pennsylvania.

However, we have deep concerns that the current program is both expensive and ineffective. 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. We noted deficiencies in selection and training of the behavior detection officers. 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, we continue to have questions with regard to the program and this fiscal year will conduct a Verification Review, with regard to—among other things—performance management, training, and financial accountability, and selection, allocation, and performance of the Behavior Detection Officers.

Likewise, the Federal Air Marshal Program costs the American taxpayer over \$800 million per year. The program was greatly expanded after 9/11 to guard against a specific type of terrorist incident. In the intervening years, terrorist operations and intentions have evolved. We will be auditing the Federal Air Marshal Program this year to determine whether the significant investment of resources in the program is justified by the risk.

*TSA's role as regulator*

TSA has dual responsibilities, one to provide checkpoint security for passengers and baggage and another to oversee and regulate airport security provided by airport authorities. The separation of responsibility for airport security between TSA and the airport authorities creates a potential vulnerability in safeguarding the system. The concern about which entity is accountable for protecting areas other than checkpoints has come up in relation to airport worker vetting, perimeter security, and cargo transport. We have also assessed whether TSA is appropriately regulating airports, such as whether it ensures airports' compliance with security regulations. We have found shortfalls.

In the case of airport worker vetting, for example, TSA relies on airports to submit complete and accurate aviation worker application data for vetting. In a recent audit, we found TSA does not ensure that airports have a robust verification process for criminal history and authorization to work in the United States, or sufficiently track the results of their reviews. TSA also did not have an adequate monitoring process in place to ensure that airport operators properly adjudicated credential ap-



plicants' criminal histories. TSA officials informed us that airport officials rarely or almost never documented the results of their criminal history reviews electronically. Without sufficient documentation, TSA cannot systematically determine whether individuals with access to secured areas of the airports are free of disqualifying criminal events.

As a result, TSA is required to conduct manual reviews of aviation worker records. Due to the workload at larger airports, this inspection process may look at as few as 1 percent of all aviation workers' applications. In addition, inspectors were generally reviewing files maintained by the airport badging office, which contained photocopies of aviation worker documents rather than the physical documents themselves. An official told us that a duplicate of a document could hinder an inspector's ability to determine whether a document is real or fake because a photocopy may not be matched to a face and may not show the security elements contained in the identification document.

Additionally, we identified thousands of aviation worker records that appeared to have incomplete or inaccurate biographic information. Without sufficient documentation of criminal histories or reliable biographical data, TSA cannot systematically determine whether individuals with access to secured areas of the airports are free of disqualifying criminal events, and TSA has thus far not addressed the poor data quality of these records. (*TSA Can Improve Aviation Worker Vetting (Redacted)*, OIG-15-98, June 2015)

Further, the responsibility for executing perimeter and airport facility security is in the purview of the 450 local airport authorities rather than TSA. There is no clear structure for responsibility, accountability, and authority at most airports, and the potential lack of local Government resources makes it difficult for TSA to issue and enforce higher standards to counter new threats. Unfortunately, intrusion prevention into restricted areas and other ground security vulnerabilities is a lower priority than checkpoint operations.

#### CONCLUSION

Making critical changes to TSA's culture, technology, and processes is not an easy undertaking. However, a commitment to and persistent movement towards effecting such changes—including continued progress towards complying with our recommendations—is paramount to ensuring transportation security. We recognize and are encouraged by TSA's steps towards compliance with our recent recommendations. Without a sustained commitment to addressing known vulnerabilities, the agency risks compromising the safety of the Nation's transportation systems.

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

#### APPENDIX A.—RECENT OIG REPORTS ON THE TRANSPORTATION SECURITY ADMINISTRATION

*Covert Testing of the TSA's Passenger Screening Technologies and Processes at Airport Security Checkpoints (Unclassified Summary)*, OIG-15-150, September 2015  
*Use of Risk Assessment within Secure Flight (Redacted)*, OIG-14-153, June 2015  
*TSA Can Improve Aviation Worker Vetting (Redacted)*, OIG-15-98, June 2015  
*The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program*, OIG-15-86, May 2015  
*Allegation of Granting Expedited Screening through TSA PreCheck Improperly (Redacted)*, OIG-15-45, March 2015  
*Security Enhancements Needed to the TSA PreCheck Initiative (Unclassified Summary)*, OIG-15-29, January 2015  
*Vulnerabilities Exist in TSA's Checked Baggage Screening Operations (Unclassified Spotlight)*, OIG-14-142, September 2014

#### APPENDIX B.—STATUS OF RECOMMENDATIONS FOR SELECTED OIG REPORTS ON TSA (AS OF 9.22.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-11-47 .....	DHS Department-wide Management of Detection Equipment.	3/2/2011	We recommend that the Deputy Under Secretary for Management reestablish the Joint Requirements Council.	Closed .....	Agreed.
OIG-11-47 .....	DHS Department-wide Management of Detection Equipment.	3/2/2011	We recommend that the Deputy Under Secretary for Management: Establish a commodity council for detection equipment, responsible for: Coordinating, communicating, and, where appropriate, strategically sourcing items at the Department level or identifying a single-source commodity manager; Standardizing purchases for similar detection equipment; and Developing a data dictionary that standardizes data elements in inventory accounts for detection equipment.	Closed .....	Agreed.
OIG-12-06 .....	Transportation Security Administration Penetration Testing of Advanced Imaging Technology.	11/21/2011	Recommendation includes Sensitive Security Information.	Closed .....	Agreed.
OIG-12-06 .....	Transportation Security Administration Penetration Testing of Advanced Imaging Technology.	11/21/2011	Recommendation includes Sensitive Security Information.	Closed .....	No Response.
OIG-12-06 .....	Transportation Security Administration Penetration Testing of Advanced Imaging Technology.	11/21/2011	Recommendation includes Sensitive Security Information.	Closed* .....	Agreed.
OIG-12-06 .....	Transportation Security Administration Penetration Testing of Advanced Imaging Technology.	11/21/2011	Recommendation includes Sensitive Security Information.	Closed* .....	Agreed.

OIG-12-06 .....	Transportation Security Administration Penetration Testing of Advanced Imaging Technology.	11/21/2011	Recommendation includes Security Information.	Closed .....	Agreed.
OIG-12-06 .....	Transportation Security Administration Penetration Testing of Advanced Imaging Technology.	11/21/2011	Recommendation includes Security Information.	Closed .....	Agreed.
OIG-12-06 .....	Transportation Security Administration Penetration Testing of Advanced Imaging Technology.	11/21/2011	Recommendation includes Security Information.	Closed .....	Agreed.
OIG-12-06 .....	Transportation Security Administration Penetration Testing of Advanced Imaging Technology.	11/21/2011	Recommendation includes Security Information.	Closed .....	Agreed.
OIG-13-91 .....	Transportation Security Administration's Screening of Passengers by Observation Techniques.	5/29/2013	We recommend that the Assistant Administrator, Office of Security Capabilities develop and implement a comprehensive strategic plan for the Screening of Passengers by Observation Techniques (SPOf) program that includes— Mission, goals, objectives, and a system to measure performance; A training strategy that addresses the goals and objectives of the SPOf program; A plan to identify external partners integral to program success, such as law enforcement agencies, and take steps to ensure that effective relationships are established; and, A financial plan that includes identification of priorities, goals, objectives, and measures; needs analysis; budget formulation and execution; and expenditure tracking.	Closed .....	Agreed.

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-13-91 .....	Transportation Security Administration's Screening of Passengers by Observation Techniques.	5/29/2013	We recommend that the Assistant Administrator, Office of Security Capabilities develop and implement controls to ensure completeness, accuracy, authorization, and validity of referral data entered into the Performance Measurement Information System.	Closed .....	Agreed.
OIG-13-91 .....	Transportation Security Administration's Screening of Passengers by Observation Techniques.	5/29/2013	We recommend that the Assistant Administrator, Office of Security Capabilities develop and implement a plan that provides recurrent training to Behavior Detection Officer (BDO) instructors and BDOs.	Closed .....	Agreed.
OIG-13-91 .....	Transportation Security Administration's Screening of Passengers by Observation Techniques.	5/29/2013	We recommend that the Assistant Administrator, Office of Security Capabilities develop and implement a plan to assess BDO instructor performance in required core competencies on a regular basis.	Closed .....	Agreed.
OIG-13-91 .....	Transportation Security Administration's Screening of Passengers by Observation Techniques.	5/29/2013	We recommend that the Assistant Administrator, Office of Security Capabilities monitor and track the use of BDOs for non-SPOT related duties to ensure BDOs are used in a cost-effective manner and in accordance with the mission of the SPOT program.	Closed .....	Agreed.

OIG-13-91 .....	Transportation Security Administration's Screening of Passengers by Observation Techniques.	5/29/2013	We recommend that the Assistant Administrator, Office of Security Capabilities develop and implement a process for identifying and addressing issues that may directly affect the success of the SPOT program such as the selection, allocation, and performance of BDOs.	Closed .....	Agreed.
OIG-13-99 .....	Transportation Security Administration's Screening Partnership Program.	6/20/2013	We recommend that the Transportation Security Administration Deputy Administrator expedite developing and implementing procedures to ensure that decisions on Screening Partnership Program applications and procurements are fully documented according to applicable Department and Federal guidance.	Closed .....	Agreed.
OIG-13-99 .....	Transportation Security Administration's Screening Partnership Program.	6/20/2013	We recommend that the Transportation Security Administration Deputy Administrator establish and implement quality assurance procedures to ensure that the most relevant and accurate information is used when determining eligibility and approving airports' participation in the Screening Partnership Program.	Closed .....	Agreed.
OIG-13-120 ....	Transportation Security Administration's Deployment and Use of Advanced Imaging Technology.	9/16/2013	We recommend that the Deputy Administrator, Transportation Security Administration: Develop and approve a single, comprehensive deployment strategy that addresses short- and long-term goals for screening equipment.	Closed .....	Agreed.

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-13-120 ...	Transportation Security Administration's Deployment and Use of Advanced Imaging Technology.	9/16/2013	We recommend that the Deputy Administrator, Transportation Security Administration: Develop and implement a disciplined system of internal controls from data entry to reporting to ensure PMIS data integrity.	Closed* .....	Agreed.
OIG-14-142 ...	(U) Vulnerabilities Exist in TSA's Checked Baggage Screening Operations.	9/9/2014	This recommendation is Classified ...	Closed .....	Agreed.
OIG-14-142 ...	(U) Vulnerabilities Exist in TSA's Checked Baggage Screening Operations.	9/9/2014	This recommendation is Classified ...	Open—Resolved .....	Agreed.
OIG-14-142 ...	(U) Vulnerabilities Exist in TSA's Checked Baggage Screening Operations.	9/9/2014	This recommendation is Classified ...	Closed* .....	Agreed.
OIG-14-142 ...	(U) Vulnerabilities Exist in TSA's Checked Baggage Screening Operations.	12/16/2014	This recommendation is Classified ...	Open—Resolved .....	Agreed.
OIG-14-142 ...	(U) Vulnerabilities Exist in TSA's Checked Baggage Screening Operations.	12/16/2014	This recommendation is Classified ...	Open—Unresolved ...	Agreed.
OIG-14-153 ...	Use of Risk Assessment within Secure Flight.	9/9/2014	Recommendation includes Security Information.	Open—Resolved .....	Agreed.**
OIG-14-153 ...	Use of Risk Assessment within Secure Flight.	9/9/2014	Recommendation includes Security Information.	Closed .....	Agreed.
OIG-14-153 ...	Use of Risk Assessment within Secure Flight.	9/9/2014	Recommendation includes Security Information.	Closed* .....	Agreed.**
OIG-15-29 .....	Security Enhancements Needed to the TSA PreCheck™ Initiative.	1/28/2015	Recommendation includes Security Information.	Open—Unresolved ...	Disagreed.
OIG-15-29 .....	Security Enhancements Needed to the TSA PreCheck™ Initiative.	1/28/2015	Recommendation includes Security Information.	Open—Resolved .....	Agreed.
OIG-15-29 .....	Security Enhancements Needed to the TSA PreCheck™ Initiative.	1/28/2015	Recommendation includes Security Information.	Open—Resolved .....	Agreed.

OIG-15-29 .....	Security Enhancements Needed to the TSA PreCheck™ Initiative.	1/28/2015	Recommendation includes Security Information.	Sensitive	Open—Resolved .....	Agreed.
OIG-15-29 .....	Security Enhancements Needed to the TSA PreCheck™ Initiative.	1/28/2015	Recommendation includes Security Information.	Sensitive	Open—Resolved .....	Agreed.**
OIG-15-29 .....	Security Enhancements Needed to the TSA PreCheck™ Initiative.	1/28/2015	Recommendation includes Security Information.	Sensitive	Open—Resolved .....	Agreed.
OIG-15-29 .....	Security Enhancements Needed to the TSA PreCheck™ Initiative.	1/28/2015	Recommendation includes Security Information.	Sensitive	Open—Resolved* .....	Agreed.
OIG-15-29 .....	Security Enhancements Needed to the TSA PreCheck™ Initiative.	1/28/2015	Recommendation includes Security Information.	Sensitive	Closed* .....	Agreed.**
OIG-15-29 .....	Security Enhancements Needed to the TSA PreCheck™ Initiative.	1/28/2015	Recommendation includes Security Information.	Sensitive	Open—Resolved .....	Agreed.**
OIG-15-29 .....	Security Enhancements Needed to the TSA PreCheck™ Initiative.	1/28/2015	We recommend that the TSA Assistant Administrator for the Office of Intelligence and Analysis: Employ PreCheck™ passengers to standard security lane screening at random intervals.	Open—Resolved* .....	Agreed.**	
OIG-15-29 .....	Security Enhancements Needed to the TSA PreCheck™ Initiative.	1/28/2015	Recommendation includes Security Information.	Sensitive	Closed* .....	Agreed.
OIG-15-29 .....	Security Enhancements Needed to the TSA PreCheck™ Initiative.	1/28/2015	Recommendation includes Security Information.	Sensitive	Closed* .....	Agreed.
OIG-15-29 .....	Security Enhancements Needed to the TSA PreCheck™ Initiative.	1/28/2015	We recommend that the TSA Assistant Administrator for the Office of Security Operations: Develop and implement a strategy to address the TSA PreCheck™ lane covert testing results.	Open—Resolved .....	Agreed.**	
OIG-15-29 .....	Security Enhancements Needed to the TSA PreCheck™ Initiative.	1/28/2015	Recommendation includes Security Information.	Sensitive	Open—Resolved .....	Agreed.**

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-15-29 .....	Security Enhancements Needed to the TSA PreCheck™ Initiative.	1/28/2015	We recommend that the TSA Assistant Administrator for the Office of Intelligence and Analysis: Provide an explanation of TSA PreCheck™ rules and responsibilities to all enrollment center applicants and include this information in eligibility letters.	Open—Resolved .....	Agreed.
OIG-15-29 .....	Security Enhancements Needed to the TSA PreCheck™ Initiative.	1/28/2015	We recommend that the TSA Assistant Administrator for the Office of Intelligence and Analysis: Coordinate with Federal Government and private partners to ensure all TSA PreCheck™ eligible populations receive the rules and responsibilities when notifying participants of eligibility.	Open—Resolved .....	Agreed.**
OIG-15-29 .....	Security Enhancements Needed to the TSA PreCheck™ Initiative.	1/28/2015	We recommend that the TSA Chief Risk Officer: Develop consolidated guidance outlining processes and procedures for all offices involved in the TSA PreCheck™ initiative.	Open—Resolved .....	Agreed.
OIG-15-45 .....	Allegations of Granting Expedited Screening through TSA PreCheck Improperly (OSC File No. DI-14-3679).	3/16/2015	Recommendation includes Sensitive Security Information.	Open—Unresolved ...	Disagreed.



OIG-15-45 .....	Allegations of Granting Expedited Screening through TSA PreCheck Improperly (OSC File No. DI-14-3679).	3/16/2015	We recommend that the TSA Assistant Administrator for Security Operations: Modify standard operating procedures to clarify Transportation Security Officer (TSO) and supervisory TSO authority to refer passengers with TSA PreCheck boarding passes to standard screening lanes when they believe that the passenger should not be eligible for TSA PreCheck screening.	Closed* .....	Agreed.
OIG-15-86 .....	The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program.	5/6/2015	We recommend that TSA's Office of Security Capabilities and Office of Security Operations develop and implement a preventive maintenance validation process to verify that required routine maintenance activities are completed according to contractual requirements and manufacturers' specifications. These procedures should also include instruction for appropriate TSA airport personnel on documenting the performance of Level 1 preventive maintenance actions.	Open—Resolved* .....	Agreed.
OIG-15-86 .....	The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program.	5/6/2015	We recommend that TSA's Office of Security Capabilities and Office of Security Operations: Develop and implement policies and procedures to ensure that local TSA airport personnel verify and document contractors' completion of corrective maintenance actions. These procedures should also include quality assurance steps that would ensure the integrity of the information collected.	Open—Resolved* .....	Agreed.

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-15-86 .....	The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program.	5/6/2015	We recommend TSA's Office of Acquisition enhance future screening equipment maintenance contracts by including penalties for non-compliance when it is determined that either preventive or corrective maintenance has not been completed according to contractual requirements and manufacturers' specifications.	Open—Resolved* ..... Agreed.	

\*These recommendations were either resolved or closed within the last 6 months.

\*\*TSA management changed their response from disagreed to agreed.

## APPENDIX C.—CURRENT AND PLANNED OIG WORK ON TSA

## PROJECTS IN-PROGRESS

Project Topic	Objective
TSA Security Vetting of Passenger Rail Reservation Systems.	Determine the extent to which TSA has policies, processes, and oversight measures to improve security at the National Railroad Passenger Corporation (AMTRAK).
Reliability of TWIC Background Check Process.	Determine whether the screening process for the Transportation Worker Identification Credential program (TWIC) is operating effectively and whether the program's continued eligibility processes ensure that only eligible TWIC card holders remain eligible.
TSA's Security Technology Integrated Program (STIP).	Determine whether TSA has incorporated adequate IT security controls for passenger and baggage screening STIP equipment to ensure it is performing as required.
TSA's Controls Over Access Media Badges.	Identify and test selected controls over access media badges issued by airport operators.
TSA's Risk-Based Strategy	Determine the extent to which TSA's intelligence-driven, risk-based strategy informs security and resource decisions to protect the traveling public and the Nation's transportation systems.
TSA's Office of Human Capital Contracts.	Determine whether TSA's human capital contracts are managed effectively, comply with DHS's acquisition guidelines, and are achieving expected goals.

## UPCOMING PROJECTS

Project Topic	Objective
Federal Air Marshal Service's Oversight of Civil Aviation Security.	Determine whether the Federal Air Marshal Service adequately manages its resources to detect, deter, and defeat threats to the civil aviation system.
TSA Carry-On Baggage Penetration Testing.	Determine the effectiveness of TSA's carry-on baggage screening technologies and checkpoint screener performance in identifying and resolving potential security threats at airport security checkpoints.
Airport Security Capping Report.	Synthesize the results of our airport security evaluations into a capping report that groups and summarizes identified weaknesses and root causes and recommends how TSA can systematically and proactively address these issues at airports Nationwide.
TSA's Classification Program.	Determine whether TSA is effectively managing its classification program and its use of the Sensitive Security Information designation.
TSA's Office of Intelligence and Analysis.	Determine whether TSA's Office of Intelligence and Analysis is effectively meeting its mission mandates.

Mr. KATKO. Those questions are indeed forthcoming, but before that Mr. Roth, I want to thank you for your testimony. I appreciate you being here.

I want to hear from our second witness, Administrator Neffenger, who I am sure the honeymoon is indeed over. You were confirmed in June 2015 as the sixth administrator of the TSA. You lead the security operations at more than 450 airports within the United States, and a workforce of almost 60,000 employees. Prior to joining TSA, Administrator Neffenger served admirably as the 29th vice commandant of the U.S. Coast Guard, and the Coast Guard's

deputy commandant for operations. The Chair now recognizes Admiral Neffenger for his testimony.

**STATEMENT OF THE HONORABLE PETER NEFFENGER, ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY**

Admiral NEFFENGER. Thank you, and good afternoon Chairman Katko, Ranking Member Rice, distinguished Members of the subcommittee, and thank you for the opportunity to testify on my vision for answering these concerns and evolving the Transportation Security Administration.

As you noted, Mr. Chairman, TSA was founded from crisis, and has continued to evolve throughout its existence. Careful and sustained oversight by Congress, and audits by the Inspector General and GAO are critical elements of this process, and I am a strong supporter of such. I thank you for the support each of you has provided in exercising that oversight. I also want to thank Inspector General Roth for identifying areas for improvement in TSA. I met with him prior to my confirmation and met with him again during my first month as administrator to relay the seriousness with which I take his work. His team has been invaluable in helping us to identify the root causes of the recent covert testing results, and I thank him for his encouraging assessment of our new direction.

That direction is a reflection of my vision on how we approach the continuing evolution of TSA. As you noted, I am now 3 months into the job, and during that time, I have traveled to about 15 airports and numerous Federal Air Marshal offices across the country. I have also visited our partners in the United Kingdom, France, and the Netherlands, and I met with our stakeholders from the airlines, travel industry, and airport operators from major airports, including Los Angeles, Atlanta, Dallas, and Chicago. I have also been engaging with surface stakeholders and passenger rail and light rail both here and in Europe.

Throughout all of these visits, I have been thoroughly impressed with the professionals who occupy our ranks. I am speaking specifically of our front-line transportation security officers. In addition to our air marshals, our inspectors, and other employees, each of whom swore an oath to serve their Nation in a mission that encounters nearly 2 million travelers a day in the aviation sector alone. I have been impressed with the collaboration I have seen across the transportation enterprise and I am pleased that the range of capabilities our Federal, State, and local partners bring to bear across every sector.

These complex systems require that we systematically examine them and consider them as a whole; that we integrate this wide range of public and private capabilities, that we benchmark and apply best practices across the enterprise, and that we seek global consistency.

I can assure you that as we move forward, we remain an intelligence-driven, risk-based counterterrorism agency with a well-defined statement of mission, clear and unequivocal standards of performance, training, and resourcing that enabled the workforce to achieve success, and a relentless pursuit of excellence and accountability.

We will conduct counterterrorism operations with discipline and competence. We will invest in deliberately developing our workforce, and we will field advance capabilities responsive to a pervasive and dynamic threat. We have a no-fail mission, one for which the consequences of a successful attack overwhelm the risk equation and for which we must ensure we deliver mission success.

My immediate priority is to pursue solutions to the recent covert testing failures and I believe we are making significant progress in doing so. In response to the IG's findings, we have implemented an action plan to ensure leadership accountability, improve alarm resolution, increase effectiveness and deterrence, increase threat testing, and strengthen our procedures.

We have also responded vigorously to Secretary Johnson's 10-point plan to review and assess screening operations, including training for the entire screening workforce, testing and improving the technology, and implementing these new procedures. We will continue to implement this plan of action and provide regular updates to you and to the Secretary.

Of utmost concern is determining root causes for the failures noted. Our conclusion is that the screening effectiveness challenges were not merely a performance problem, nor were they a failure of the advanced imaging technology. Indeed, this technology has greatly enhanced our ability to detect threats and it continues to perform to expected standards when deployed and used properly.

Strong drivers of the problem, however, include leadership focus, environmental influences, and gaps in system design and processes along with a disproportionate focus on efficiency and speed in screening operations rather than security and effectiveness. These powerfully influenced organizational culture and officer performance. As a result, there was significant pressure to clear passengers quickly at the risk of not diligently resolving alarms.

Our analysis also revealed our officers did not fully understand the capabilities and limitations of the equipment and several procedures were inadequate to resolve alarms. We have trained our officers to understand and use the equipment properly and we have corrected our procedures. Solutions require a renewed focus on security, streamlined effective procedures, investments in technology, and realistic, consistent, standardized training along with a new balance between effectiveness and efficiency. We must support our officers as they perform their duties.

We will continue to partner with our airlines and other members of the travel and airport industry to ensure that we can reduce stress on the checkpoint and we will right-size and re-source TSA appropriately. Our near-term solutions will halt further reductions in officer staffing to support our revised screening efforts, provide consistent high-quality training at a centralized location, and enhance our technology.

Our Mission Essentials Training conducted over the past 2 months with every front-line officer and leader across TSA has helped to reset our focus on security effectiveness, and most critically, has enhanced our officers' knowledge of the screening systems that they operate.

I refer repeatedly how valuable this information is to our officers. I need to now extend that into our new-hire training across the

country. We need greater consistency and efficiency in its delivery, and we must do more to establish a professional foundation that is required of a high-performing counterterrorism organization.

As such, I am committed to expanding our existing TSA Academy at the Federal Law Enforcement Training Center and plan to send all new-hire TSOs to basic training beginning in January 2016. Centralized training in a formal, professional academy ensures consistency and professionalism, produces greater enthusiasm, increased confidence and skills, and connectedness to a common agency culture and focus on mission.

We must ensure the appropriate measures of effectiveness are in place to drive an institutional focus on our primary mission. We must employ a culture of operational evolution, one that constantly reassesses assumptions, plans, and processes, so we are able to rapidly field new concepts of operation and we must deliver an effective system and earn the confidence of the traveling public through competence, discipline, performance, and professionalism.

We face a critical turning point in evolving TSA, both to address these recent findings and begin our investment in a strategic approach to securing the transportation sector. As such, I am committed to ensuring that we do so, that we employ multiple elements in intelligence-driven operations, while discarding a one-size-fits-all approach that we recruit and retain a highly-trained workforce, with accountability and high standards of performance.

Chairman Katko, Ranking Member Rice, we have an incredible challenge ahead of us, but I know that TSA is up to the task. I thank you for the opportunity to appear before you today, and I look forward to your questions.

[The prepared statement of Admiral Neffenger follows:]

PREPARED STATEMENT OF PETER NEFFENGER

OCTOBER 8, 2015

Good afternoon Chairman Katko, Ranking Member Rice, and distinguished Members of the subcommittee. Thank you for the opportunity to testify on my vision for evolving the Transportation Security Administration (TSA).

Since its creation following the terrorist attacks of September 11, 2001, TSA has played an invaluable role in protecting the traveling public. Fourteen years after the 9/11 attacks, we face threats more dangerous than at any time in the recent past. Terrorist groups and aspiring violent extremists, inspired by messages of hatred and violence, remain intent on striking our Nation's aviation system as well as other transportation modes. The threat is decentralized, diffuse, and quite complex.

These persistent and evolving threats are TSA's most pressing challenge and require an intense and sustained focus on our security missions. We remain deeply committed to ensuring that TSA remains a high-performing, risk-based intelligence-driven counterterrorism organization. We are working diligently to ensure we recruit, train, develop, and lead a mission ready and highly-capable workforce, placing a premium on professional values and personal accountability. Further, we will pursue advanced and innovative capabilities that our mission requires to deter, detect, and disrupt threats to our Nation's transportation systems, with a clear understanding that we must continue to optimize today's capabilities while envisioning future methods of achieving success.

I am intently focused on leading TSA strategically, developing and supporting our workforce, and investing appropriately, to deliver on our vital security mission.

IMPROVING AVIATION SCREENING OPERATIONS

My highest priority for TSA is determining root causes and implementing solutions to address the recent covert testing of TSA's checkpoint operations and technology conducted by the Department of Homeland Security (DHS) Office of Inspector

General (OIG). I was greatly disturbed by TSA's failure rate on these tests, and have met with the Inspector General on several occasions to better understand the nature of the failures and the scope of the corrective actions needed.

Screening operations are a core mission of TSA. In fiscal year 2014, our officers screened approximately 660 million passengers and nearly 2 billion carry-on and checked bags. Through their diligent daily efforts, our officers prevented over 180,000 dangerous and/or prohibited items, including over 2,200 firearms, from being carried onto planes. In addition, our workforce vetted a daily average of 6 million air passengers against the United States Government's Terrorist Screening Database, preventing those who may wish to do us harm from boarding aircraft, and conducting enhanced screening of passengers and their baggage prior to allowing them to board an aircraft. In conjunction with these screening efforts, and using intelligence-driven analysis, TSA's Federal Air Marshals also protected thousands of flights. To ensure compliance with aviation security requirements, in fiscal year 2014 TSA Inspectors completed over 1,054 airport inspections, nearly 18,000 aircraft operator inspections, and almost 3,000 foreign air carrier inspections to ensure compliance with aviation security requirements. Still, as recent and prior testing shows, we must continue to formulate solutions that will enhance our effectiveness at checkpoint screening operations.

It is important to acknowledge that the OIG covert tests, as a part of their design, focused on a discrete segment of TSA's myriad capabilities of detecting and disrupting threats to aviation security. TSA conducts similar, more extensive testing that is part of a deliberate process designed to defeat and subsequently improve our performance, processes, and screening technologies. TSA's covert testing program, along with the OIG's covert testing, provides invaluable lessons learned, highlighting areas in which the agency needs improvement in detecting threats. Such testing is an important element in the continual evolution of aviation security.

As we pursue solutions to the challenges presented by recent and on-going covert testing, there are several critical concepts that must be in place. TSA must ensure that its value proposition is well-defined, clearly communicated, understood and applied across the entire workforce and mission enterprise. From my first day on the job, I have made it clear that we are first and foremost a security organization. Our mission is to deter, detect, and disrupt threats, and we must ensure every officer, inspector, air marshal, and member of our agency remains laser-focused on this mission. In addition, we must ensure the appropriate measures of effectiveness are in place to drive an institutional focus on the primary security objectives for all modes of transportation, and renewed emphasis on aviation measures.

We have demonstrated our ability to efficiently screen passengers: However, it is clear that we now must improve our effectiveness. By focusing on the basic fundamentals of security screening, and by readjusting the measurements of success to focus on security rather than speed, and by measuring what we value most, we can adjust the institutional focus and adapt the culture to deliver success. TSA must adopt a culture of operational evolution, one that constantly questions assumptions, plans, and processes, and is able to rapidly field new concepts of operation, performance standards and capabilities, particularly given the persistent and adaptive enemy we face.

To drive these important changes, it is essential to understand and assess appropriately the effectiveness of our aviation security enterprise, to rigorously pursue initiatives to quickly close capability and security gaps, and employ our own covert testing and vulnerability assessments. Delivering an effective security system and earning the confidence of the traveling public will come only through competence, disciplined performance, successful results, and professionalism. These imperatives are essential to address the immediate challenges, and more broadly, to accomplish the important mission entrusted to TSA.

In late May, in response to the OIG initial findings, TSA developed and implemented an immediate action plan built on its understanding of the known vulnerabilities in checkpoint operations. Consisting of dozens of individual actions, it was designed to:

- (1) ensure leadership accountability;
- (2) improve alarm resolution;
- (3) increase effectiveness and deterrence;
- (4) increase threat testing to sharpen officer performance;
- (5) strengthen standard operating procedures;
- (6) improve the Advanced Imaging Technology (AIT) system;
- (7) deploy additional resolution tools; and
- (8) improve human factors, including enhanced training and operational responses.

Scheduled for completion in March 2016, TSA is actively engaged in implementing this plan of action and provides regular updates to the Secretary of Homeland Security as well as frequent updates to the Congress.

There are a number of immediate actions that have been completed, including the following: (1) Requiring screening leadership at each airport to oversee AIT operations to ensure compliance with standard procedures; (2) requiring each officer to complete initial video-based training to reinforce proper alarm resolution conversations; (3) conducting leadership and officer same-day debriefs for threat inject testing and lessons learned; and (4) performing daily operational exercises and reinforcement of proper pat-down procedures at least once per shift to ensure optimal TSO performance.

#### SECRETARY JOHNSON'S TEN-POINT PLAN

In addition to the TSA action plan, Department of Homeland Security Secretary Jeh Johnson directed a series of actions, which in cooperation with TSA, constituted a 10-point plan to address these findings. TSA is now working aggressively to accomplish these actions. The plan includes the following:

- Briefing all Federal Security Directors at airports Nation-wide on the OIG's preliminary test results to ensure leadership awareness and accountability. This was completed in May and continues regularly. In September, I convened the leadership of TSA—from across the agency and in every mission area—to discuss our progress, to clearly convey my expectations, and to outline my vision for the evolution of our counterterrorism agency.
- Training every Transportation Security Officer (TSO) and supervisor to address the specific vulnerabilities identified by the OIG tests. This training also is intended to reemphasize the value and underscore the importance we place on the security mission. The training will reemphasize the threat we face, the design of our security system, integrating technology with human expertise, the range of tools we employ to detect threats, and the essential role our officers perform in resolving alarms. Fundamentally, this training is intended to explain the “why” behind our renewed and intense focus on security effectiveness. We are also training supervisors and leaders to ensure they appreciate and support the shift in emphasis. Most important, we are asking our supervisors to recognize their critical role in supporting our officers' renewed focus on alarm resolution. This training began May 29, 2015 and was recently completed at the end of September 2015.
- Increasing manual screening measures, including reintroducing hand-held metal detectors to resolve alarms at the checkpoint. This has been underway since mid-June and reinforces our ability to detect the full range of threats.
- Increasing the use of random explosives trace detection, which also started in mid-June, enhancing detection capabilities to a range of threat vectors.
- Re-testing and re-evaluating screening equipment to measure current performance standards. We are retesting the systems in the airports tested by the Inspector General and assessing performance of the field systems against those in the labs to ensure optimal performance. This testing, which began in June and is on-going, will help us to more fully understand and strengthen equipment performance across the enterprise.
- Assessing areas where screening technology equipment can be enhanced. This includes new software, new operating concepts, and technology upgrades in collaboration with our private-sector partners.
- Evaluating the current practice of including non-vetted populations in expedited screening. We continue to take steps to ensure that we have a more fully-vetted population of travelers exposed to screening in our expedited lanes. For example, as of September 12, the practice of Managed Inclusion–2 is no longer used in daily operations.
- Revising TSA's standard operating procedures to include using TSA supervisors to help resolve situations at security checkpoints. On June 26, 2015, TSA began field testing new standard operating procedures at six airports. Lessons learned



will be incorporated and deployed Nation-wide. This procedure is intended to ensure appropriate resolution techniques are employed in every situation.

- Continuing covert testing to assess the effectiveness of these actions. For each test, there must be a same-day debrief with the workforce of outcomes and performance along with immediate remediation actions. Expansion of our testing also enhances officer vigilance.
- Finally, we have responded vigorously by establishing a team of TSA and other DHS officials to monitor implementation of these measures and report to the Secretary and me every 2 weeks. These updates have been on-going since June.

#### ROOT CAUSE ASSESSMENT

DHS and TSA are also committed to resolving the root causes of these test failures. A diverse team of DHS leaders, subject-matter experts, as well as officers and leaders from the front-line workforce are examining the underlying problems resulting in our performance failures and will make recommendations on system-wide solutions for implementations across the agency.

The team's initial conclusion is that the screening effectiveness challenges noted by the Inspector General were not merely a performance problem to be solved solely by retraining our officers. Officer performance is but one among many of the challenges. TSA front-line officers have repeatedly demonstrated during their annual proficiency evaluations that they have the knowledge and the skill to perform the screening mission well. Nor was this principally a failure of the AIT technology. These systems have greatly enhanced TSA's ability to detect and disrupt new and evolving threats to aviation. AIT technology continues to perform to specification standards when maintained and employed properly, and we continue to improve its detection capabilities.

The challenge can be succinctly described as a set of multi-dimensional factors that have influenced the conduct of screening operations, creating a disproportionate focus on screening operations efficiency rather than security effectiveness. These challenges range across six dimensions: Leadership, technology, workforce performance, environmental influences, operating procedures, and system design.

Pressures driven by increasing passenger volume, an increase in checkpoint screening of baggage due to fees charged for checked bags as well as inconsistent or limited enforcement of size requirements for hand-carried bags and the one bag plus one personal item (1+1) standard<sup>1</sup> create a stressed screening environment at airport checkpoints. The challenges also include the range of complex procedures that we ask our officers to employ, resulting in cognitive overload and personnel not properly employing the technology or a specific procedure. The limitations of the technology, the systems detection standards, TSA officers' lack of training on equipment limitations, and procedures that failed to resolve the alarms appropriately all undermined our ability to effectively screen, as noted by the Inspector General's report.

A critical component of the problem was confusing messages on the values of the institution, as expressed in the metrics used to assess effectiveness and leadership performance. As noted, a prior focus on measures that emphasized reduced wait times and organizational efficiency powerfully influenced screening performance as well as organizational culture. As a result, across TSA, leaders' and officers' organizational behavior emphasized efficiency outcomes and a pressure to clear passengers quickly, at the risk of not diligently resolving alarms. The combined effect of these many variables produced the performance reported by the Office of the Inspector General.

#### IMPLEMENTING SOLUTIONS

Solutions to the challenges facing TSA will require a renewed focus on the agency's security mission, a commitment to right-sizing and re-sourcing TSA to effectively secure the aviation enterprise, and an industry commitment to incentivizing vetting of passengers as well as creating conditions that can decrease the volume and contents of bags presented for screening in airports.

<sup>1</sup>The Aircraft Operator Standard Security Program, Dated October 21, 2013, requires, with some exceptions for crewmembers, medical assistance items, musical instruments, duty-free items, and photographic equipment, that the accessible property for individuals accessing the sterile area be limited to one bag plus one personal item per passenger (e.g., purse, briefcase, or laptop computer).

For TSA, we must renew our focus on the fundamentals of security, thereby asking our officers and leaders to strike a new balance between security effectiveness and line efficiency, to field and diligently perform appropriate resolution procedures and to close technology and performance gaps. We need our managers and supervisors to support our officers when they perform their difficult daily mission. As we move forward, we are guided by a principled, strategic approach, with specific projects already underway to advance our goal of ensuring we deliver on our mission to deter, detect, and disrupt threats to aviation.

This principled approach extends beyond the immediate findings identified in the OIG's covert test of checkpoint operations. This approach also informs our strategy and ability as an agency to systematically evolve operations, workforce development, and capability investment, now and in the future. We will systematically review the prior findings of OIG and GAO reports as well as other sources of analysis that can inform security effectiveness.

#### *Redefine Value Proposition*

First, TSA is in the process of ensuring our focus on security effectiveness is well-defined and applied across the entire workforce and mission space. Our "Mission Essentials—Threat Mitigation" course, being provided to every officer by the end of September, is our initial step. We will follow this initial effort with a range of initiatives to convey these priorities to leaders and officers using additional tools, such as a statement of the Administrator's Intent, the National Training Plan, and in our workforce messaging. Redefining our values as an agency by focusing on threat mitigation and improving TSO awareness and knowledge of the threat will provide a new and acute mission focus. Resolving every alarm, with discipline, competence, and professionalism are the values we are emphasizing to the workforce. From my initial field visits, I can report that our officers are hearing, understanding, and applying this new approach.

#### *Communicate New Standards and Expectations*

To communicate these new standards, TSA's Office of Intelligence and Analysis is pursuing an information-sharing project to expand and ensure standardized information and intelligence sharing to front-line officers. Expanding the reach of the threat information provided to the field, enhancing our officers' awareness and understanding of the threat and the critical role they play in interdicting these threats creates ownership and a greater commitment to ensuring security procedures are followed.

#### *Align Measures of Effectiveness to Standards and Expectations*

TSA's Office of Security Operations is examining and revising the current Management Objectives Report to rebalance the field leaders' scorecard with security effectiveness measures in addition to some preserved efficiency data. We are operating on the premise that what we measure are the organizational objectives to which our field leaders will pay close attention. We expect the first iteration of our new measures to be in the field by early October 2015.

#### *Design System to Achieve Desired Outcome*

The aviation security system must interdict the full range of threats on the Prohibited Items List and evolving threats that require our immediate action. Our concept of operations review project, run by the Operations Performance and Mission Analysis Divisions, is further identifying system-wide gaps and vulnerabilities and how to ensure the traveling public is exposed to our mission-essential detection capabilities when transiting the screening checkpoint. The results of this analysis may lead to a range of recommended improvements, from clarification of pat-down procedures to fielding decisions for new technologies.

#### *Eliminate Gaps and Vulnerabilities in Achieving Desired End-State*

Our work in analyzing the root causes has identified a range of vulnerabilities in TSA; however, there is no single office or accountable official charged with systematically tracking our vulnerability mitigation efforts. Centralizing these activities under a single official should drive systemic research, development, and fielding of new capabilities. Our TSA Office of the Chief Risk Officer is managing this project.

#### *Evaluate Performance by Using the New Values, Standards, and Expectations*

To motivate behavior, supervisors must clearly communicate the performance objectives they expect from their subordinate officers and leaders. Our Chief of Human Capital is working an initiative we are calling the "Performance Evaluation Project," which is designed to ensure the appropriate focus on desired mission outcomes is

imbedded within Annual Performance Plans. These new standards will be used for the performance period that started on October 1, 2015.

*Incentivize Performance to Enact Values, Standard, and Expectations*

Several of our field leaders and officers have also recommended a *Model Transportation Security Officer Project* to determine model performance criteria. The project is intended to incentivize performance and emphasize the values and standards front-line employees are expected to uphold across the enterprise. I am a strong proponent of incentivizing performance, as this can be a powerful instrument to drive employee behaviors. Through these efforts, we intend to convey our values, measure them, and evaluate performance against these new expectations, uniting the TSA workforce behind critical agency reforms that will deliver organizational alignment and strengthen our security posture.

Finally, we will continue to partner with the trade and travel industry, the airlines, and airport operators to identify solutions that can fundamentally alter the reality on the ground for our screening workforce.

A key element of our solution set will be reassessing the screening workforce staffing baseline. Budgeted staffing levels for fiscal year 2016, planned more than a year in advance of the covert testing failures, presumed a significant increase in the vetted traveling population which, combined with Managed Inclusion, allowed for a smaller workforce. We are reassessing screener workforce staffing needs and planning additional adjustments to support training and operational enhancements, all to ensure future staffing reductions remain rational choices that balance effectiveness with efficiency. Additionally, we look forward to working with the Congress to identify means of adding additional field intelligence officers to ensure every field operation is supported with a dedicated intelligence officer to facilitate information sharing, and to expand our efforts at the TSA Academy to train the workforce. Finally, we expect to invest in Advanced Imaging Technology detection upgrades based on the OIG findings.

#### MISSION ESSENTIALS TRAINING

Given the importance of training to our mission, I would like to elaborate on TSA's approach to training following the OIG covert testing results. It is critical that we train out these failures so we do not repeat the mistakes, including those which could have catastrophic consequences. As of October 1, we have trained the specifics of the failures to virtually every front-line member and leader of TSA.

This training, referred to as "Mission Essentials—Threat Mitigation," builds our workforce understanding of the link among intelligence, technology, and the procedures they perform. The training advances our new value proposition by: (1) Providing a detailed intelligence briefing on the current threat; (2) discussing passenger tactics and techniques that may be used to dissuade the TSOs from thoroughly performing their screening duties and what counter-measures they can employ; (3) reviewing recent procedural changes for screening individuals who present themselves as having a disability; (4) practicing pat-down procedures with the goal of finding components of improvised explosive devices; and (5) exploring the capabilities and limitations of the checkpoint equipment and how the TSO can by following proper procedures. I have been encouraged to see our TSOs embracing the principles of Mission Essentials training.

Through this training, our employees are being taught how to respond to social engineering—techniques used by passengers seeking to manipulate our screening workforce and avoid regular processes. As I meet with these employees in my travels to airports throughout the country, I have heard repeatedly that they wished they had this valuable information. As such, I have charged TSA's senior leaders to plan to send all new-hire TSOs to the TSA Academy at the Federal Law Enforcement Training Center in Glynco, GA, for TSO-basic training beginning in January 2016. Most of our major counterterrorism partners in security and law enforcement send their employees through similar-type academies to ensure a laser-focus on mission, and we should as well. We recognize this initiative may require additional resources, and look forward to working with the committee accordingly.

#### FUTURE OF SCREENING

As we envision the future of screening, even in the context of the current challenges, I remain a strong proponent of a risk-based approach to security. The vast majority of people, goods, and services moving through our transportation systems are legitimate and pose minimal risk. To support our risk-based approach, it is critical to continue growing the population of fully-vetted travelers, such as those participating in TSA PreCheck™ or in other DHS trusted traveler programs. In par-

allel, I am also reviewing expedited screening concepts with the intent of moving away from unvetted travelers. This multi-pronged, risk-based approach will result in separating known and unknown travelers, with known travelers receiving expedited screening and other travelers, some high-threat, receiving more extensive screening.

I envision a future where some known travelers will be as vetted and trusted as flight crews. Technology on the horizon may support passengers becoming their own "boarding passes" by using biometrics, such as fingerprint scans, to verify identities linked to Secure Flight. The Credential Authentication Technology (CAT) is the first step in this process and will provide TSOs with real-time authentication of a passenger's identity credentials and travel itinerary.

A second objective is to screen at the "speed of life" with an integrated screening system that combines metal detection, non-metallic anomaly detection, shoe X-ray, and explosive vapor detection. Prototypes of these machines exist, which hold great promise for the traveling public.

Purposeful checkpoint and airport designs that facilitate screening advances are also a future approach. At Los Angeles International Airport (LAX) Tom Bradley International Terminal, recent innovative renovations have been completed so that screening operations are seamlessly integrated into the movement and flow of the traveling public. This effort will continue, with 6 out of 8 terminals at LAX scheduled for design and renovation. Other locations, such as Dulles International Airport (IAD), have dedicated checkpoints that separate expedited screening from other operations, allowing TSOs to follow the appropriate concepts of operations with greater focus and clarity.

While some airports may not be able to take the same approach, the future of screening is based on fulfilling the promise of risk-based security. By increasing the number of fully-vetted passengers and enhancing the effectiveness and efficiency of physical screening, I am committed to refining and advancing our risk-based security strategy. I look forward to working with this committee and the Congress to chart a way forward in this regard.

#### CONCLUSION

Chairman Katko, Ranking Member Rice, we have an incredible challenge ahead of us. Still, I know TSA is up to the task, and will adjust its focus from one based on speed and efficiency to one based on security effectiveness. We are on the front lines of a critical counterterrorism fight and our workforce is willing and able to do the job. I thank you for the opportunity to appear before you today and sincerely appreciate your time and attention. I look forward to your questions.

Mr. KATKO. Thank you, Administrator Neffenger.

I called you Admiral or Administrator, either one. It is interchangeable, I guess. But thank you again for your testimony. I appreciate the fact that you are responding rapidly, and recognizing, and embracing the problems, and trying to find solutions. I am encouraged by that. We all are. We look forward during the course of the questioning here today to talk about moving forward, what is the plan, and we hope you weave that into your testimony as we go through it today.

I also thank you for rearranging your schedule to be here with us today. I now recognize myself for 5 minutes to ask questions.

I will start by observing the nature and tenor of this hearing and how it is different from the other ones that we have had. The other hearings we have had so far, and we have had 7 subcommittee hearings. This is the seventh one, I believe, which is more than any in all of Homeland Security, and perhaps more than most in Congress. The reason is because there is a lot to do. There is a lot of issues to examine.

At the forefront of examining of those issues has been the Inspector General, and we appreciate that. Like we said earlier, by Miss Rice, I believe, or someone, more than 100 such reports have been done by the Inspector General since the inception of TSA. Those reports are revealing and also at times troubling. Since we got into

the hearings this year, we did one on the Atlanta gun trafficking case which exposed 170 guns being trafficked by employees through supposedly secure access points. It exposed a major weakness in the airline aviation system and that is employee access controls, which are sorely lacking. That was exacerbated by a number of cases recently in Dallas/Fort Worth, and LAX, and Oakland, and elsewhere where major drug trafficking rings had been disrupted.

One of those rings, at the preliminary hearing, one of the employees was bragging about the fact that he could bring anything through there, including a bomb, which is incredibly troubling. Instead of having an oh-my-God-moment by the airports, we hear a lot of pushback about costs, and that is something we are going to have to examine going forward. We have had a lot of hearings about screenings and the problems with screenings, a 97 percent fail rate in recent tests. That is unbelievably troubling.

We have had hearings about PreCheck and Managed Inclusion and how people are getting pulled out of regular lines into the PreCheck line without any additional background checks, which defeats the purpose of PreCheck.

We have heard about the Federal Air Marshal Service and we had a good productive hearing with them and then we found out that after that, Federal Air Marshals are filling sessions with prostitutes in hotels paid for with Government credit cards, and Lord knows what else is going on. That is troubling too.

We have also heard some things about private screenings from the Inspector General. This all points up that, I think, and underscores the belief by the Inspector General himself that sometimes—and it is not on your watch, Mr. Neffenger, but sometimes, many times, TSA has not responded. That leads me to the conclusion that TSA, while a young agency, has become a very bureaucratized agency already, too slow to respond and not nimble enough to respond.

So the genesis of all that was why I had this hearing today to allow us to discuss at a more general level what are some of its systemic problems that we see at TSA, and we are doing this to benefit Mr. Neffenger's presence so that he can hopefully address them going forward.

So with that teeing the ball up, Mr. Roth, I would like to hear from you as to what you think some of the, you know, global problems are at TSA, and I encourage you to be as frank as possible.

Mr. ROTH. Thank you, Mr. Chairman, and let me preface my remarks by, this is a look back over a number of different audit reports that span the course of years. One of the conclusions or themes that I can draw from this is that there is a mismatch between the risk and meeting the risk. That sort of working theory that we have is either TSA doesn't understand the nature of the risk, or they do understand the nature of the risk, and then worse from that is that they don't address the risk in any appropriate way.

Again, I am going to be speaking in the past tense about this because I do think, or at least I am hopeful, consistent with my auditor's vow of critical thinking and skepticism, but I am hopeful that we are in a new era. But I will talk about three episodes that to

me sort-of illustrate one of the big issues we have in sort-of either not understanding the risk, or simply dismissing the risk.

The first is, of course, our covert testing. The recent round of covert testing was not a surprise to us and it was not a surprise to TSA. We had been doing covert testing over the years with consistently disappointing results. You know, as we like to say, the best test of a football team is how they do on Sunday. To us, a covert testing is the Sunday game. Real-world conditions, figure out exactly how well the system works, and it did not work very well.

What we found after the covert testing was even a little bit more upsetting, which was, TSA does their own covert testing and those results were very similar to our results. So none of this came as a surprise to TSA. One of the things that we discovered after this round of testing and the, I would say, the very vigorous response that the Department gave with regard to our briefing on the covert testing, was that no one in DHS had known sort-of this issue; that the issue had remained within TSA. TSA had not sort-of elevated the issue. It came as a surprise to the Secretary, to the Deputy Secretary, to the leadership within the Department.

When you look at TSA's fiscal 2016 budget, 2016 budget what it shows is that they are actually going to reduce the number of screeners. Their proposal was to reduce the number of screeners by about 1,700 people. Now, this is a budget that was developed over time and certainly not under this current administrator's watch, and I understand that it is going to be reversed, but I think it shows sort of a cultural attitude that they knew that they had a risk.

Their response to that risk was reducing the number of screeners. Their justification for it, and I am just reading from their budget document that was submitted to the Hill, was that TSA employs a multi-layered, risk-based, intelligence-driven approach to its security and counterterrorism mission, and as a result of these, they are focusing efforts on efficiency and can save money as a result of this. Which is in direct contradiction to the evidence that they had at the time as to the efficiency of checkpoint operations.

So they either dismissed the risk, or understood the risk, but, yet, didn't meet the risk. So that would be the first episode, and if I could have, there is a couple of others, which I am happy to continue, or—

Mr. KATKO. Yeah, for a few moments, please.

Mr. ROTH. Okay. The second one is our audit on PreCheck. You know, we had real concerns about Managed Inclusion and PreCheck. As you know, you had a hearing on this. I had a conversation with the previous administrator about our audit report where we had deep concerns that people that didn't have an individualized assessment of risk were getting expedited screening. His answer was, well, look, it is my job to accept the risk, and I am accepting this risk, which is fine, except my family flies. So, you know, I am not sure that is an adequate answer. That all of these people went through Secure Flight.

So the idea is, of course, that they have been vetted against certain intelligence databases to determine whether they are a risk. I mean the problem with that is any student of modern terrorism history understands that 17 of the 19 9/11 hijackers were unknown

to the intelligence community, and they wouldn't be on any sort of special list.

Richard Reid, the shoe bomber was not on any special list. The Christmas day bomber in 2009 was not on any list. The most significant terrorist attack we had in recent memory, the Marathon bomber, Tamerlan Tsarnaev, wasn't on any list. In fact, he was looked at by the FBI and adjudged not to be a threat and then not on any sort of active list.

So this idea that, oh, well, it is an intelligence-based, and that is the silver bullet, and that is what is going to help us here, is just a wrong-headed assessment of risk. As I said, again, this was not on this administrator's watch, but it was very deeply upsetting to me during the course of our audits to see this kind of a reaction.

Mr. KATKO. Thank you, Mr. Roth. I will have some questions for you, Admiral Neffenger, on the second go-around if we are able to get to that. If not, I will ask you to submit the questions in writing depending on our schedule here.

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

Miss RICE. Thank you, Mr. Chairman. Inspector General Roth, what I would like to ask you, you mentioned in your statement the No. 1 thing is that TSA can do to change the culture, which is what you cite as significantly problematic. So what are your thoughts on how you change the culture?

Mr. ROTH. Okay, it is a difficult problem, because it is a problem that has grown up over time. One of the ways that you change the culture is, I think, what the administrator is currently doing, which is an honest look at what it is that is going on and sort of honestly confront your problems and put a plan of action in place.

Historically, it has not been that. It has been both for us and GAO sort-of a reaction, and a very disturbing reaction, for example, in our covert testing I think for 2012, we had our results and TSA pushed back considerably on our methodology, and on a number of other things. But lo and behold, they had their own internal testing that was almost the same. So what kind of an agency is sort of pushing back in public, and yet, understands that the audit is correct?

As I said, I think this is changing, and there is an honest assessment of what is going on. My understanding is that the administrator is going to put forth a realistic strategic plan that isn't, you know, everything is wonderful and we are doing fine, and pay no attention to the man behind the curtain, but rather this is a problem. The risks of catastrophic terrorism are real, and we absolutely need to get it right.

So it is a long process. There isn't a single magic bullet, but certainly, good leadership helps and that is what we are hopeful for.

Miss RICE. So being 1 of 10 kids, I have to be optimistic, right, and I am choosing to be optimistic about the ability to change the culture at TSA because it has only been around for a short period of time, right? I am on the Veterans Affairs' Committee and I can tell you that that agency does the same exact thing. Every time there is an IG report that says here is a problem, here is a problem, they push back and say no, no, no, there is no problem. Noth-

ing needs to be changed. The stakes are equally high for both our veterans, right, and National security, domestic, and international that TSA is dealing with.

So I am glad to hear you, Mr. Roth, speak so bluntly because that is what we need. That is what your job is, but I am also happy to hear that you are optimistic about Admiral Neffenger, because I am very optimistic about the new administrator for a whole host of reasons.

So one issue that I do want to address because you mentioned this, because I do believe, Mr. Roth, that in order to do an adequate assessment of your risk, right, intelligence has to be part of that. One of the things that I was so distressed to hear about, is how the TSA is responsible for doing the checks on airport employees, and yet, they are given incredibly poor information to do these background checks, which affects the ability to really adequately assess the risk of this employee, which as the Chairman pointed out, when you have gunrunners and drug runners, some of whom are employed by the agency, that is problematic.

So my question is to you, Admiral Neffenger, regarding that—it seemed to me that that was a fix that didn't have to be a legislative fix. You, as the administrator, could say, from now on, if you want a background check to be done, which you have to have done, these are the things—these are the pieces of information that we need to get, or you don't get the background check and you can't hire the person.

So just that one area, if you could just address that one issue?

Admiral NEFFENGER. Yes, thank you. With respect to that, so I have got some good news to report. We actually get access to a whole host of information in databases now that allow us to do—and actually, we always had access to terrorist screening database, and databases with known or suspected terrorist information in it.

Some of which you are referring to are some categories within what is called the terrorist information datamart environment. It is just a big database where this was information that may or may not be sufficient to directly tie somebody to a known or suspected terrorist, or identify them as such, or there might be partial information. Those are the categories that we had, you know, one-by-one, or case-by-case access to, but not automated access. So we have asked for that automated access and we are working through the interagency to achieve that.

We have also dramatically improved our oversight of the airport vetting environment. So as you know, we still vet the folks who are applying for secure access badges. But to the Inspector General's point, we had not been overseeing the collection of information and the maintenance of the data in doing regular audits of that. We are doing that now directly as a result of the Inspector General's findings.

So I think that we are moving forward in a good way on getting information. I share your concern that we have access to as much information as we need to have access to in order to fully vet people who we put into trusted environments, given what we have already known about what has happened in some of the airport environments across the country. I think that we made good progress.



I have met with my counterparts in the intelligence community, and I have been sitting—I met with the National security staff and the senior directors for trans-border and others to make clear my priorities, and so far I have been getting good results from that.

Miss RICE. Great, thank you both very much.

Mr. KATKO. Thank you, Miss Rice. The Chair now recognizes the Ranking Minority Member of the Homeland Security Committee, the gentleman from Mississippi, Mr. Thompson.

Mr. THOMPSON. Thank you very much, Mr. Chairman. Administrator Neffenger, one of the real challenges I alluded to in my opening statement went toward the fact that we buy technology in the form of equipment for vulnerabilities that they can't detect. How are you going to close that gap between known vulnerabilities and acquiring equipment and technologies that won't detect it?

Admiral NEFFENGER. Well, you know, Mr. Thompson, you really hit on a key concern, and that is how do you get beyond today's security systems and look towards the future and evolve fast enough to meet what we know to be an evolving threat environment? I think there are a couple of things we need to do.

First of all, I would like to see more robust competition in the marketplace. Right now we are tied to a couple of key vendors. They have done good work and they produced some good equipment for us, but I would like to see even more competition. I would like to incentivize more. I think there is a lot of creativity in the private sector and I think there is a lot of innovation in the private sector.

I have got some thoughts on ways in which we can incentivize that competition to include small business competition because I think that some of the small businesses out there are doing some of the most innovative work that we have.

The second piece is to have a clear understanding of what the threat is so that when we develop the requirements that we need for the equipment that we are looking for, that those requirements are expansive and robust; that we don't just look to buy the next thing on the shelf that looks like it might do the job, but that you have got to really start—I will back up a moment because it speaks to some of the points that each of you have made with respect to focus on mission.

You really have to start with the mission. It is not just enough to say my mission is secure. You have to say, well, what does that mean? What are the components of my mission? So you have to do a true analysis of the mission. I say this sincerely, I start every day by thinking about the mission and I work backwards from there and I think, what does it take to accomplish this mission? What are the requirements we need to—if you are sitting at a checkpoint, what does that checkpoint have to actually do? What is the nature of the threats that might present themselves at the checkpoint? How might you determine those threats? How might they be presented? In what manner can they be presented? All of the different variations of that. That is a very complex process to do that, but you have to do it, and you have got to dissect that mission down to the—down to the details.

Then you can begin to put out requirements that I think we can—we will see much more robust response to that. In the mean

time, I want to make sure that the equipment that we currently operate is operating to its peak. So we are working to get the most out of the current equipment as we look to move the next technology in.

Mr. THOMPSON. Well, and not for a response, if we keep buying current equipment that can't identify those known vulnerabilities, we are not where we need to be, and I think this robust competition is healthy because when you only have three major players in the area, you know, that is a lot. So I look forward to your leadership to incentivize other competition. I think that is important. We put it in the legislation, and I hope that authority gets us where we need to be.

A couple of other things. You talked about the checkpoints. You know, TSOs are special to a lot of the traveling public. Most of the time, that is all people see are those men and women at the checkpoints. I would like to make sure that those men and women are being encouraged to be the best that they can be, and not penalized. Now, I heard something yesterday and I just need a yes or no answer. Are the medical guidelines for TSOs and all other employees for TSA the same?

Admiral NEFFENGER. You know, I don't know the answer to that question exactly, because I am looking at the very medical guidelines right now. I know that they have over the past year, before I became confirmed, I know that we had been working on updating the standards for medical guidelines. Here is what I believe to be the case. That I think that there are different categories of medical guidelines depending upon the type of work that you have to do in the organization.

For example, I believe that there are certain physical standards you have to be able to meet in order to perform the duties as a baggage check person that may or may not be the same standards that you have to hold if you are an employee at TSA headquarters.

Mr. THOMPSON. I want you to check that out.

Admiral NEFFENGER. But I will verify it for you.

Mr. THOMPSON. Because I am told that, like, people who are TSOs who might have asthma get discharged by having asthma, or high blood pressure, diabetes, whatever; but that people in management somehow don't. Actually, I have the information, but that is a problem from my vantage point because if you have a different—just look at that.

Admiral NEFFENGER. I will do that.

Mr. THOMPSON. In health. I have got some other questions that I will submit, Mr. Chairman, for the record to get it. But I would also like unanimous consent to provide for the record that there have been 165 TSOs who have been terminated for disqualifying medical conditions—and cancer. I mean, you know, how can you terminate somebody because they have cancer? I mean, that is, you know, what I am saying? So I don't want us to be a scrooge. I want us to treat people humanely, and I would like to include that into the record.

Mr. KATKO. Without objection, so ordered.

[The information follows:]

LIST SUBMITTED FOR THE RECORD BY RANKING MEMBER BENNIE G. THOMPSON

TSO'S REMOVED/TERMINATED FOR DISQUALIFYING MEDICAL CONDITIONS FOR CALENDAR  
YEAR 2014—THE NUMBER OF TSO REMOVALS/TERMINATIONS IS 165

Breakdown By Gender:

Female—85

Male—80

Total—165

*Breakdown by Disqualifying Medical Guideline*

- Anxiety Related Dysfunction—15
- Arrhythmias—1
- Arthritis—2
- Asthma—3
- Behavior Dyscontrol—1
- Bipolar Disorder—2
- Body Mass Index—1
- Cancer—3
- Cardiomyopathy, Myocarditis, Constrictive Pericarditis—2
- Cataracts, Corneal Disorder, Eye Disorders—1
- Cervical, Thoracic and Lumbosacral Disc Disease Syndrome—23
- Chronic Bronchitis, Cystic Lung Disease & COPD—1
- Chronic Pain—4
- Coronary Artery Disease—1
- Delusional/Paranoid Dysfunction—1
- Depression Related Disorder—13
- Diabetes Mellitus—3
- Equilibrium Disorder—3
- Gout—1
- Hernia—1
- Hip, Knee, Ankle and Foot Related Dysfunction—4
- Hypertension—1
- Inability to Lift and Carry Items Weighing up to 70 Pounds—19
- Inability to Walk, Stand for Periods Greater Than 10 Minutes—1
- Inflammatory Bowel Disease—1
- Irritable Bowel Syndrome—5
- Lumbar Spine Disorder—5
- Lumbosacral Surgery—1
- Migraines and Other Episodic Headaches—18
- Mobility and Dexterity—3
- Motor Neuron Disease—1
- Osteoarthritis—4
- Pain & Neuropathies—1
- Parkinson's Disease—1
- Peak Expiratory Flow (PEF)—1
- PTSD—2
- Renal Function—1
- Seizure Disorder—6
- Sleep Disorder—2
- Spinal Abnormalities—1
- Transient Neurological Events—1
- Traumatic Brain Injury—1
- Vertigo—2
- Visual Acuity Far And Near—1

Total=165

TSOS REMOVED/TERMINATED FOR DISQUALIFYING MEDICAL CONDITIONS FOR CALENDAR  
YEAR 2013—THE NUMBER OF TSO REMOVALS/TERMINATIONS IS 185

Breakdown By Gender

Female—106

Male—79

Total—185

*Breakdown by Disqualifying Medical Guideline*

- (1) Migraines and Other Episodic Headaches—27
- (2) Anxiety—14
- (3) Depression and Related Disorder—10

- (4) Cervical Lumbar—1
- (5) Diabetes—9
- (6) Inflammatory Bowel Disease—3
- (7) Anemia—1
- (8) Anticoagulation Therapy—1
- (9) Psychotic Functioning—1
- (10) Cervical Thoracic—12
- (11) Gout—3
- (12) Urticaria—1
- (13) Joint Condition—3
- (14) Heart Disease—2
- (15) Cancer—2
- (16) Ventricular Arrhythmia—2
- (17) Inability to Lift and Carry Items Weighing up to 70 Pounds—44
- (18) Inability to Squat and Bend—6
- (19) Inability to Walk, Stand for Periods Greater Than 10 Minutes—8
- (20) Mobility and Dexterity—9
- (21) Vertigo—1
- (22) Inguinal, Umbilical or Ventral Hernia—1
- (23) Endocrine Disorder—1
- (24) Chronic Pain—4
- (25) Myotonic Dystrophy—1
- (26) Renal Dysfunction—1
- (27) Peripheral Neuropathy—1
- (28) Spinal Abnormalities—2
- (29) Sleep Disorder—2
- (30) Meniere's Disease—1
- (31) Asthma—1
- (32) Seizures—2
- (33) Chronic Bronchitis—2
- (34) Diplopia and Visual Field Loss—1
- (35) Delusional/Paranoid Dysfunction—1
- (36) Behavioral Dyscontrol—2
- (37) Syncope—1
- (38) Thoracic Outlet Synedrome—1

Total—185

Mr. KATKO. Thank you, Mr. Thompson. The Chair now will recognize other Members of the committee for questions they may wish to ask the witnesses.

In accordance with the committee rules and practice, I plan to recognize Members who were present at the start of the hearing by the seniority on the subcommittee. Those coming in later will be recognized in the order of arrival.

The Chair now recognizes Mr. Keating from Massachusetts for 5 minutes of questioning.

Mr. KEATING. Thank you, Mr. Chairman. It was only me, anyway.

Mr. KATKO. Well, you are very important to all of us.

Mr. KEATING. Thank you, sir. Thank you for being here Mr. Roth, Inspector General Roth, and thank you for your work. You are talking about a culture. Let me just do this again. You know, it is not just TSA administrator that we are talking about in terms of the culture. It is higher up, Secretary Ridge when he was a witness, I brought this up with him, and he agreed it was a major issue.

Secretary Napolitano, when she was the Secretary several times said this is a priority. It is an issue. I brought it up with Secretary Johnson, and last summer I brought it up with you. You agreed that this was a top priority. That is the issue of perimeter security around the airports. I have been saying this for so long and the re-

sponse has been to cut down the number of vulnerability studies and to tell this committee that things are more secure.

In the mean time, teenagers, intoxicated people, are breaching perimeter security, go right up to the aircraft, which is, I hate to say this publicly, but which is an amazing target. They can put a bomb on there the same way that these teenagers had access and not even risk their own lives the way people would ordinarily have to do it if they are going to breach the gate.

So I wanted to follow up, No. 1, with that question to see what steps have been taken since we last discussed this, and what you expect to implement.

The second issue, part of the problem with perimeter is the jurisdictional issue. You have got some airports that are municipal airports, very small airports, but still networked into the big commercial flights. You have got authorities, all kinds of brands and shapes, all types of resources to deal with it. The continuing problem of what to do with the exit lanes, which TSA maintains is still a priority, it is still important.

It is still an access point, but you want to shift that authority to these airports that aren't even doing the job with perimeter security.

So the two questions I have are: What is the update on perimeter security in terms of implementing what you said was high priority? No. 2, how can we resolve the exit lane issue which I think if it is so important for TSA, it should remain their responsibility and make sure we have the kind of security we need there, because that is a vulnerability standpoint as far as I have seen? If you could, those two questions, Administrator Neffenger, and thank you again for making yourself so available.

Admiral NEFFENGER. Yes, sir, thank you, Mr. Keating.

Perimeter security, as you know, one of the things that was requested right in the aftermath of the Atlanta issue was a look by the Aviation Security Advisory Committee at vulnerabilities across the airport system. I think that provided a very good series of issues to address as well as some strong recommendations and we have been working to, first of all, to think about how to implement those, and then to take a good solid look at the system.

So it actually is a significant priority of ours to ensure perimeter security. I share your same concerns with it. So what have we done? I have ordered a look at all of the airports across the country.

I want to know from top to bottom, you know, what have we done with respect to perimeter security, including access control points, how those access control points are maintained, and then what do we do to actually ensure the safety and security of the perimeter itself? What is the nature of the perimeter, and how consistently is it enforced around? So that is a fairly large undertaking, and I haven't seen the results of that request yet.

The other thing I am doing is putting more effort into that oversight piece. We have legislative authority to do that oversight whether you are dealing with a local airport authority, a local municipality, or a large aviation concern. All of it falls under the purview, and I think that there are—you can set clear performance standards for how that is done.

So the first is to assess what the current state really is as opposed to—

Mr. KEATING. I don't want to interrupt you, but my time is going away on me. Do you have a time frame in which that study could be taking place? I am a few weeks away from asking this question for 6 years now. Do you have a time frame?

Admiral NEFFENGER. Well, I understand your frustration so we are doing that right now. Let me get you an actual time frame so that I—because I don't want to promise something I can't deliver on a certain time, but I can commit to you is that it is happening right now and I have asked the same question.

I am very concerned about the same issue, I want you to understand. Because that system is important. Let's say you get the checkpoint 100 percent right. There are more vulnerabilities in the aviation system than the checkpoint.

Mr. KEATING. The exit lane, briefly if you could.

Admiral NEFFENGER. I will get back to you on the exit lane question as well, sir.

Mr. KEATING. Thank you. I yield back.

Mr. KATKO. Thank you, Mr. Keating. We are getting ready for votes, but I think what I would like to do, if any of the other Members have questions, just ask questions and have you respond to the rest in writing. I have a few that I would like to have responded to in writing before we wrap up here.

With respect to Mr. Roth, simply, Mr. Roth, if there are other kind of 30,000-foot observations you would like to make about TSA that you weren't able to cover today in the short period that we were here, I encourage you to submit them in writing to the committee and I encourage you to be as blunt and open as possible. I think it is important to expose that, and make sure to copy the administrator on it as well.

With respect to Administrator Neffenger, there are a couple of things I would like to have you talk about. Ranking Member Thompson hit it right on the head with the technology issues. One of the things he said that is very important is he said he has only seen three major players, if you will, within the technology providing for the administration, and that sometimes it seems like there is a sense of comfort with dealing with just those three.

I think competition is a good thing. I have been to many technology presentations recently and the updated technology out there is stunningly advanced. It seems to me that I would like to hear from you, actually, as to what you are doing to vet that technology, and how you are encouraging these newcomers on the scene to give them a fair shake. Not only from a competition aspect, but taking a real good hard look at everything from the prescreening aspects with the biometric data, to the actual physical screening procedures and machines because we know there are problems with them now, and going forward, how are you going to address that?

The other component I want to ask you about is the age of the screening equipment itself. Because from my understanding, much of this equipment is at or near a 10-year lifespan. That I would like to know what the plans are going forward to replace it because many of these are at the end of their lifespan and—projected life-

span at least, and it doesn't seem like there is a plan going forward on the horizon.

So I would like to see what the blueprint is going forward to deal with this new technology. I think Mr. Thompson is 100 percent right that technology is critically important and hearing from all parties, not just the ones that TSA is comfortable with. That is very important.

Let me make sure there is nothing else here. Oh, yeah, last thing is, with respect to the access controls. I would like to hear what has been done since we have to tighten up access controls, and I will note to just warn you that with respect to the Viper team that was celebrated as a risk-based security for the access controls, but it was completely exploited by the individuals in the Dallas/Fort Worth case.

As a matter of fact, employees went into areas and if the Viper team was there, they just simply called out to their comrades to bring the drugs and contrabands to another exit, another entry point. That is a major concern. So I don't want to hear too much about the Viper teams because it is not getting the job done. It's pretty obvious. They are a good idea, but they are easily circumvented. So I would like to hear what your ideas are about that going forward, and what has actually been done going forward.

I really look forward to getting that bill passed that we just recently passed out of the House and getting it signed—passed out of the Senate and signed by the President so that we can get to work on doing an in-depth study that is really needed with this.

So with that, I will ask my colleagues if they have any further questions they want to have submitted for the record. Anything?

All right, if there is anything further, we will submit them to you in writing within 10 days.

I thank you very much. It was an abbreviated session, but we have had a few things going on today as you might imagine, and it is now time for some votes. So thank you very much.

[Whereupon, at 4:08 p.m., the subcommittee was adjourned.]





## APPENDIX

---

### QUESTIONS FROM CHAIRMAN JOHN KATKO FOR PETER NEFFENGER

*Question 1.* The Transportation Security Administration (TSA) has long been plagued with accusations of mismanagement and waste. Since taking the helm at the agency, have you had the opportunity to assess the various programs and activities in TSA's area of responsibility and identify any areas that are in need of reform, restructuring, or elimination?

Answer. On an annual basis, the Transportation Security Administration (TSA) examines all programs and activities to review current requirements and execution of resources along with program performance to ensure optimal use of limited resources. This process identifies realignments, restructurings, and/or elimination of programs or activities to propose in the annual Congressional budget submission.

Over the past several fiscal years, TSA has identified efficiencies and savings in the budget. For example, in fiscal year 2014, TSA identified approximately \$100 million in various enterprise-wide and administrative/professional support contract efficiencies; in fiscal year 2015 and 2016, TSA's budget submissions reflected over \$200 million in savings as a result of implementing risk-based security initiatives. Realignments have also been made through the formal budget process to better apportion resources to TSA's organization and management structure, while enhancing mission effectiveness. In the fiscal year 2015 budget, TSA permanently consolidated the Federal Air Marshal Service Appropriation into a single Program, Project, and Activity (PPA) within TSA's Aviation Security Appropriation and realigned the Intelligence PPA from Transportation Security Support Appropriation to the Intelligence and Vetting Appropriation.

TSA recently established a new level of review in the budget process for the fiscal year 2018–2022 cycle which will include in-depth, transparent, agency-wide program reviews and prioritization of requirements. In the current fiscal climate, TSA will ensure that the available resources are effectively and efficiently aligned and managed to minimize waste. Additionally, TSA will ensure that programs and activities support the TSA and Department of Homeland Security's (DHS) missions, while aligning resources to the TSA Administrator's and DHS Secretary's priorities.

Programs and activities are also assessed when high-priority emergent needs arise outside of the development of an annual budget. For example, TSA initiated a programmatic review of security procedures addressing issues raised by the DHS Office of Inspector General (OIG) covert testing results issued in May 2015. The report revealed the need for improvements in the screening process, to be addressed in the near and long terms. Based on the review, resource realignments have been proposed to improve security performance and monitoring. TSA is committed to optimizing resources, and remaining a high-performing, risk-based intelligence-driven agency.

*Question 2.* How do you plan to measure and evaluate TSA's success in achieving programmatic goals and outcomes?

Answer. The Transportation Security Administration (TSA) will report strategic and management measures externally through the Future Years Homeland Security Program system. These select measures align to the Department of Homeland Security Mission 1.1 Goal: Prevent Terrorism and Enhance Security. TSA will also use other metrics to measure the effectiveness and efficiency of individual security programs, such as the use of scorecards to assess performance management in the Measures of Effectiveness (MOE) report. This report identifies security programs, procedures, and technology deemed strategically important by TSA leadership, and measures performance at the airport, regional, and National levels. The MOE replaces the previous Management Objectives Report and reflects the increased emphasis on security effectiveness and a decreased emphasis on throughput. The specific performance metrics used in the MOE reporting are organized into the following four broad categories:

- *Workforce Readiness*.—Measures emphasize the continued development of an adaptive and flexible counterterrorism workforce that is highly-trained, competent, and ready to meet the threat.
- *System Readiness*.—Measures improve mission effectiveness by measuring the implementation and continuation of risk-based, intelligence-driven security initiatives aimed at deterring and disrupting adversary activity.
- *Workforce Performance*.—Measures reflect the ability of TSA's human assets to detect threats to aviation security presented through the screening checkpoint and checked baggage.
- *System Performance*.—Measures reflect the operational and management conditions that optimize TSA's ability to detect threats to aviation security.

Individual programs will also have management-level reports which measure all facets of those programs, procedures, and/or technologies.

*Question 3.* Do you believe that TSA is adequately adapting its tactics and resources to mitigate the evolving threats to transportation? Similarly, do you believe TSA's foreign partners are keeping up with threats emanating from overseas? How has TSA improved its overseas footprint and coordination with other governments?

Answer. The Transportation Security Administration (TSA) identifies key risk information related to global aviation, conducts systematic analysis to determine key risk drivers, and develops effective and efficient strategies that mitigate the inbound aviation risk to the United States. TSA assesses the security posture at international airports that serve U.S. aircraft operators and from which foreign air carriers serve the United States. TSA has made great strides in strengthening its international network by developing and instituting an innovative risk management methodology that drives the allocation of resources and operations to target the most important vulnerabilities. TSA identifies these vulnerabilities and determines how frequently an airport should be assessed based on existing data collection and analysis. In fiscal year 2015, TSA conducted 146 foreign airport assessments and 289 air carrier inspections.

TSA relies on a wide range of activities, resources, and personnel to effect change in the vulnerability posture at a foreign airport. TSA determines a way forward, choosing from a number of direct or indirect mitigation actions. When a specific threat is identified or significant vulnerabilities warrant additional mitigation actions, TSA may issue Security Directives and Emergency Amendments to be implemented by air carriers at selected locations. Following issuance of these Security Directives or Emergency Amendments, TSA relies on a number of methods, such as ad hoc visits or inspections, to verify compliance with the additional measures. Follow-up assessments and inspections reveal whether any reduction in vulnerability occurred. The results of these visits enable TSA to determine if the mitigation actions were successful.

TSA also aligns its strategic engagements with international partners using this risk-based approach. Through its TSA Representatives and International Industry Representatives, as well as through TSA Senior Leadership engagement, TSA is able to influence and inform key decision makers in both foreign governments and industry on on-going threat streams and associated vulnerabilities in the aviation security system, and encourage a subsequent mitigation strategy to address these vulnerabilities. TSA, through its internationally-deployed workforce, builds and maintains relationships with foreign government officials, foreign and domestic air carriers, civil aviation authorities, airport authorities, international aviation organizations, and other U.S. Government stakeholders to enhance global aviation security. In addition, TSA plays an active role in the International Civil Aviation Organization, and engages with a number of regional international aviation security working groups, such as the Quadrilateral Working Group, where TSA coordinates with other Member States on a range of pressing aviation security issues, and mitigation measures.

TSA continues to examine its international footprint to ensure that it has the appropriate resources forward-deployed to mitigate the inbound threat. Since 2013, TSA has opened two new offices in Africa—Senegal and Morocco—bringing the total to four offices on that continent.

*Question 4.* Subsequent to the OIG's report release, Secretary Johnson announced that a "Tiger Team" of DHS and TSA officials would monitor the implementation of measures put in place to improve security at airport checkpoints. The committee requests that a copy of the "Tiger Team" report is transmitted to Congress upon completion. By what date do you expect this report to be completed?

Answer. We expect the report to be complete and available to the committee not later than November 25, 2015.

*Question 5.* Technology plays an important role in mitigating evolving threats to transportation security. Traditionally, TSA has engaged the same vendors in the

procurement process which has hampered competition and innovation. What is being done by TSA to engage with new vendors and encourage increased competition in the procurement process?

Answer. Almost all of the Transportation Security Administration's (TSA) contracts are awarded competitively through open-source procurements. However, there are only a limited number of vendors with capabilities sufficient enough to satisfy TSA's very specific mission-related requirements. TSA actively participates—both in a leading and supporting role—in recurring industry engagement events to promote transparency, and provide input on topics such as key operational issues, process improvement, and procurement forecasting. TSA encourages robust competition as it ultimately reduces risk to the Government and increases vendor performance.

In addition, TSA frequently works with small businesses interested in accessing the market and was pleased to make a significant award to a small business. In March 2015, TSA awarded a contract for 1,170 Explosives Trace Detection (ETD) units to a new Small Business entrant, a prime example of a small business introducing new ETD technology into aviation security and achieving approval through the TSA Qualified Products List process.

In addition, TSA employs market research by submitting requests for information, publishing broad agency announcements, and hosting industry days that help facilitate engagement with a variety of industry stakeholders, including those that are not currently TSA vendors.

Most recently, TSA issued the Transportation Security Innovative Concepts Broad Agency Announcement through *FedBizOpps.gov*, seeking to accelerate the design, realization, and delivery of new capabilities by focusing on advancing state-of-the-art technology and increasing knowledge or understanding related to transportation security.

*Question 6.* Last week, the committee released its report from the Task Force on Combating Terrorist and Foreign Fighter Travel. As I am sure you are aware, a record number of individuals are traveling to active conflict zones, and a number of these individuals return to the United States undetected. This poses a serious threat to our Nation's security.

What steps is TSA taking to address this issue? Are you actively collaborating with other relevant departments and agencies to develop strategies to combat terrorist and foreign fighter travel? How is TSA collaborating with partners abroad to identify and prevent bad actors from boarding planes bound to the United States?

Answer. The Transportation Security Administration (TSA) has a number of programs in place to identify passengers who have booked travel from abroad to the United States, and who may pose a security risk. These programs rely upon near-real-time information sharing with our stakeholders, industry partners, and the intelligence community. TSA's Secure Flight program conducts passenger watch list matching for more than 270 U.S. and foreign air carriers with flights into, out of, within, and over the United States, as well as covered U.S. flights between two international points, to identify individuals who may pose a threat to aviation or National security, and designate them for enhanced screening or prohibition from boarding an aircraft, as appropriate. TSA also provides risk-based, intelligence-driven, scenario rules to Customs and Border Protection (CBP) for use in the Automated Targeting System—Passenger to identify international travelers requiring enhanced screening based upon our knowledge of patterns identified as needing additional scrutiny.

In 2015, TSA identified a number of known or suspected terrorists who attempted to travel on commercial aircraft, and who represented the highest threat to transportation, some of whom were identified as potential foreign fighters. For these cases, TSA took action to address the threat, which included, as appropriate, denial of boarding to prevent overseas travel to participate in foreign fighting or to conduct other nefarious activities.

TSA also assigns intelligence officers to key components with responsibilities for analytical partnerships and watchlisting duties. TSA intelligence personnel are embedded at 8 different agencies and centers; these include the Department of Homeland Security Office of Intelligence and Analysis, the CBP National Targeting Center, the Terrorist Screening Center, the National Counterterrorism Center, the Central Intelligence Agency, and the National Security Agency. In these positions, TSA intelligence analysts work closely across organizational lines to optimize information-sharing efforts, and facilitate a coordinated U.S. Government response to known and suspected terrorist travel. Improved monitoring and vetting processes of travelers with robust data analytics provide a clearer understanding of travelers' movements, and permit the sharing of a superior common operating picture between agencies to mitigate potential threats.

TSA personnel are also assigned to law enforcement-related agencies and task forces to facilitate information sharing. These assignments include the Syria-Iraq Task Force, and the Federal Bureau of Investigation-led National Joint Terrorism Task Force. These officers collaborate daily with the Federal Bureau of Investigation, CBP, and other organizations to disseminate intelligence relating to foreign fighters.

Additionally, TSA Field Intelligence Officers assigned to our Nation's airports work closely with CBP, and the local Joint Terrorism Task Forces locally develop a coordinated approach to engagement with local stakeholders and coordinate intelligence messaging and threat awareness to the field, developing and maintaining a common aviation threat picture for Federal, State, and local task force officers assigned to U.S. airports, as well as TSA field components specific to foreign fighter Tactics, Techniques, and Procedures.

*Question 7.* The President recently signed into law H.R. 719, which I introduced earlier this year; this bill requires the TSA to conduct a reclassification of employees within the Office of Inspection to ensure that those employees classified as criminal investigators spend at least 50% of their time conducting criminal investigations. Those investigators spending less than 50% of their time on criminal investigations will be reclassified and receive pay that is commensurate with their actual job responsibilities. The OIG estimated that this will result in savings of approximately \$17.5 million in taxpayer dollars over 5 years. We exchanged letters on this matter this summer in which you stated that TSA and OIG are working closely together to ensure all employees are properly classified.

Can you give the committee an estimate of how long it will take to evaluate and implement this reclassification?

Answer. The Transportation Security Administration (TSA) is committed to conducting an independent full position classification review and workforce analysis to determine the appropriate classification of each position currently classified as a criminal investigator in the Office of Inspection. TSA will reclassify any criminal investigator position that does not meet the minimum legally-required 50 percent criminal investigation workload.

TSA and the Office of Personnel Management (OPM)—the recognized expert in the field of position classification and workforce analysis—have agreed to a statement of work for the classification review and workforce analysis as requested by the Office of the Inspector General (OIG). TSA currently awaits OIG final approval of the OPM methodology outlined in the statement of work to initiate the independent OPM review and analysis of the TSA Office of Inspection criminal investigations workforce.

*Question 8a.* Two weeks ago, the President signed into law H.R. 720, the Gerardo Hernandez Airport Security Act of 2015, which requires the TSA to increase communication and coordination with all pertinent agencies that would respond to an airport during a crisis situation, which was the result of a tragic event. The committee has voiced concern over the amount of training TSOs receive, as it pertains to operating technology being used at checkpoints, but I want to make sure the TSA is adequately training the TSOs to defend themselves as well. This is an officer safety issue and we simply must give the people on the front lines the tools to succeed and survive.

How much training do TSOs receive in defensive tactics?

*Question 8b.* How are the TSOs taught to deal with physically combative people at the checkpoints, who may or may not have a weapon?

Answer. While the Transportation Security Administration (TSA) currently does not offer defensive tactics training to the Officer workforce, it has taken significant steps to address employee safety concerns. Immediately following the tragic November 1, 2013, incident at Los Angeles International Airport (LAX), TSA required all its employees to complete training on how to recognize and respond to an active-threat incident in the workplace, be it an office or airport environment. TSA developed a series of interactive training courses with the support and participation of local airport officials, law enforcement officers, and TSA personnel to help Officers:

- recognize how to respond when an active shooter is in their vicinity;
- identify how to interact with Law Enforcement Officers who are responding to an incident; and
- execute the widely-accepted active-shooter response reactions of Run-Hide-Fight.

Most recently, TSA created a new training course entitled “Active Shooter Incident Response Training.” Filmed entirely at the Indianapolis (IND) airport, the interactive training video reinforces the widely-accepted active-shooter response reactions of Run-Hide-Fight. TSA released the training video in January 2015, with a required completion date of March 31, 2015. TSA mandates Active-Shooter train-

ing as an annual training requirement for its employees, and the entire TSA screening workforce has completed the training.

In addition to the active-shooter video, Operational Directive (OD) 400-19-2, Emergency Evacuation Drills, addresses the requirement for employees to be familiar with the two types of emergency evacuation drills: Controlled and uncontrolled. The evacuation drills are scenario-based and include active shooter as an uncontrolled drill. The minimum requirement is two drills per year. The reporting requirement is to document airport completion of emergency evacuation drills in the Performance Measurement Information System (PMIS) and individual employee completion in the Online Learning Center (OLC).

*Question 9.* Airport employee access controls continue to be a concerning security vulnerability. I introduced H.R. 3102, the Airport Access Control Security Improvement Act of 2015 earlier this year, and it passed the House earlier this week.

Can you please provide an update to the committee on what changes to employee access controls TSA has implemented this year? What additional changes do you have planned?

Answer. The Transportation Security Administration (TSA) performed a comprehensive review of Aviation Security Advisory Committee (ASAC) proposed recommendations regarding access controls. As a result, TSA issued Information Circular (IC) 15-01 on April 29, 2015. This IC made recommendations to airports to reduce the number of access points to the operational minimum, to increase the number of continuous random inspections for individuals entering the sterile/secured area other than through the checkpoint, and to promote a culture of situational awareness by leveraging the Department of Homeland Security's "If You See Something, Say Something" campaign, or a similar program.

On August 26, 2015, TSA issued IC 15-01A to provide further details regarding recommended inspections and measures previously identified in IC 15-01, and those measures that are mandated by TSA in the Security Directive (SD) 1542-06-01 series. This version supplied additional specific recommendations regarding the inspection of individuals, such as inspecting for a minimum number of hours per week, restricting other access points when inspections are being conducted, as well as recommendation of the methodology of the actual search.

Finally, TSA is developing a capability for continuous monitoring of airport employees' criminal history records. Once implemented, TSA will be notified of any change in an employee's status so that appropriate action can be taken. At this time, TSA is piloting this process at a limited number of airports, and intends to expand it system-wide, once completed. TSA already performs recurrent vetting against the Terrorist Screening Database.

TSA continues to work with the airports through the Federal Security Directors to ensure access points are kept to an operational minimum, and that random and unpredictable inspection of individuals and property entering the sterile/secured areas is conducted.

*Question 10.* The OIG recently issued a report that uncovered 73 aviation workers that had links to terrorism which were not detected in the initial screening process. Furthermore, the report found that different airports employed different screening techniques and there lacked consistency across the board. What is the current status of TSA's efforts to improve and streamline the employee screening process?

What additional measures do you feel are necessary in order to improve the daily screening of employees at our Nation's airports?

Answer. The Transportation Security Administration (TSA) is committed to further strengthening our ability to identify insider threats at our Nation's airports, as well as to streamline the employee-vetting process. As indicated in the Office of the Inspector General report, 69 individuals (represented by 73 records) had records in certain Governmental databases to which TSA did not have automated access when they were first vetted. These individuals have never been on the terrorist watch list. TSA recognizes the value of having as much relevant data as possible to make informed decisions in its vetting, and is pursuing access to additional types of intelligence records to maximize its vetting capabilities. TSA now requires airports to conduct a criminal history records check (CHRC) every 2 years, and will continue to do so until an alternative recurrent CHRC process is developed. TSA is working collaboratively with the Federal Bureau of Investigation (FBI) to develop and establish next generation identification databases, which would automatically update an employee's criminal history as incidents occur. TSA and FBI are moving to pilot the initiative with two airports and one airline. This initiative aligns with the Department of Homeland Security's Office of Inspector General and Aviation Security Advisory Committee (ASAC) recommendations for improving Aviation Workers security.

TSA has been working to implement many ASAC recommendations for improving the employee screening process at our Nation's airports.

These measures include:

- Working to implement the FBI/Next Generation Identification RAP Back Service, which would automatically update an employee's criminal history as events occur in order to augment the current 2-year background check process;
- Training enhancements on verification of identification documents, recognition of identity fraud, and behavioral analysis for use by Government and industry partners at the airports;
- Increasing intelligence-sharing opportunities with industry partners at the airports; and
- Examining the ASAC recommendation to develop enhanced employee access security model based on elements such as intelligence, game theory, and risk-based security principals that would cause employees to have a reasonable expectation of being inspected.

*Question 11.* Secretary Johnson stated that random screening of airport employees was increased after authorities uncovered that aviation workers in Atlanta and New York City were smuggling weapons and ammunitions. By how much was screening increased? Do you believe that this has been an effective deterrent?

Answer. In the aftermath of the Atlanta and New York City incidents, in January 2015, the Transportation Security Administration (TSA) increased the amount of random screening of employees through its Playbook Program. With Playbook, TSA personnel conduct screening on an unpredictable basis at locations throughout the airport. These activities, which include but are not limited to, identity verification, physical screening of accessible property, and explosives detection, are coordinated at the local airport level and conducted by Transportation Security Officers. Playbook operations provide a level of risk-based and unpredictable screening for Security Identification Display Area badge-holding personnel and others who are entering the airport at locations other than the screening checkpoint.

From January 1–September 30, 2015, TSA screened over 11 million employees using Playbook operations. This is a 340 percent increase compared to the 2.5 million employees screened using Playbook in the prior year.

Playbook is not the only deterrence method used to address the insider threat. TSA has worked with airports to reduce the number of access points at airports regulated by TSA to an operational minimum. TSA has also recommended and worked with airports to limit access privileges for aviation workers.

TSA believes that providing a visible presence, and additional random screening at employee access points, coupled with our other layers of security, creates an effective deterrent. TSA will continue to focus on mitigating the insider threat.

*Question 12.* In a recent response to a letter sent by the committee, TSA indicated that it was aware of allegations of sexual misconduct by Air Marshals in mid-June. Why was the committee not informed of this issue earlier, particularly in light of the oversight hearing that was held on the FAMS on July 16?

Answer. The Transportation Security Administration (TSA) is committed to working with committee staff to ensure they are kept aware of relevant investigations; however, details will not be available until investigations are complete and the circumstances surrounding the allegation(s) are known. TSA will continue to keep the committee staff up-to-date and informed.

#### QUESTIONS FROM RANKING MEMBER BENNIE G. THOMPSON FOR PETER NEFFENGER

*Question 1.* Has TSA moved forward with the implementation of changes to the dispute resolution process and the NRC without adopting any of the union's recommendations?

Answer. No, the Transportation Security Administration (TSA) has not moved forward with the implementation of changes to the dispute resolution process and the National Resolution Center (NRC) without adopting any of the Union's recommendations. The NRC, the TSA office that administers and implements the resolution process, has not made any changes to the existing resolution process. The NRC provided the American Federation of Government Employees (AFGE) a copy of the draft dispute resolution process policy for AFGE's input. AFGE provided its input and the NRC continues to consider this input and revise the draft policy. Once the NRC completes additional revisions to the draft dispute resolution process policy, another draft copy will be provided to AFGE for input before the revised policy is issued. AFGE was informed of this via email on September 29, 2015.

*Question 2.* The 2012 Determination requires that the union's suggestions be adopted "to the extent possible." Is it TSA's position that the union's suggestions were impossible to adopt?

Answer. As an initial matter, the 2011 Decision issued by former Administrator Pistole is no longer in effect. It was replaced by the 2014 Determination issued by former Administrator Pistole on December 29, 2014. In regard to the Unitary Dispute Resolution System (UDRS), the 2014 Determination does not require that TSA take the Union's suggestions to the extent possible. Instead, the 2014 Determination stipulates that the Union is encouraged to provide input, including any suggestions, comments, and/or concerns to the National Resolution Center (NRC) regarding the policy governing the UDRS as applied to covered employees. The NRC gave the Union an opportunity to provide its input on changes to the Transportation Security Administration (TSA) policy governing the UDRS and is considering its input. The NRC will give the Union another opportunity to provide further input before the policy is issued. If the NRC does not incorporate the Union's input into the TSA policy, the NRC will provide a written response to the Union explaining the basis for its decision.

*Question 3.* TSA and the union are in mediated talks for a new contract, and the union has initiated a request for informal interest-based discussions with TSA. Given the union's strenuous objections to TSA's unilateral changes to the NRC and the dispute resolution process, will TSA agree to limit the role of the NRC in accordance with the Memorandum of Agreement signed by TSA and AFGE throughout the duration of those discussions?

Answer. The current collective bargaining is for a new collective bargaining agreement on the negotiable issues listed in former Administrator Pistole's December 29, 2014, Determination on Transportation Security Officers and Collective Bargaining (2014 Determination). The NRC is the Transportation Security Administration's (TSA) office that administers and implements the dispute resolution processes for all TSA employees, not just bargaining unit employees. Only one aspect of the dispute resolution process is reflected in a Memorandum of Agreement (MOA) signed by TSA and AFGE in 2012. The MOA addresses third-party review of certain disciplinary actions and other covered disputes for bargaining unit employees. The MOA was not a part of collective bargaining in 2012 and is not a part of any collective bargaining agreement. Significantly, the MOA also does not govern or limit the NRC.

*Question 4.* Do the Medical Guidelines apply to TSA managers?

Answer. The Medical and Psychological Guidelines for Transportation Security Administration Transportation Security Officer Job Series (TSO Medical Guidelines) apply to the Supervisory Transportation Security Officers (STSOs). Management officials, other than STSOs, who manage security screeners do not fall under the TSO Medical Guidelines as physical/medical requirements have not been established for these positions.

*Question 5.* Once the exam confirms a TSO has a certain diagnosis of migraines, Type 1 or 2 diabetes or heart disease, for instance, is TSA required to establish that the medical condition impairs the ability of the TSO to perform their duties?

Is it assumed that a diagnosis or confirmation of a medical condition is in itself proof that the TSO is not fit for duty?

Answer. The Transportation Security Officer (TSO) has to meet the medical and psychological requirements of the position. Generally, it is not assumed that a diagnosis is in itself proof that the TSO is not fit for duty. The Transportation Security Administration's physician will obtain information on the TSO's medical conditions, medications, and job limitations, and will compare that information with the TSO Medical Guidelines, and may seek other sources of medical information to determine fitness for duty.

*Question 6.* TSOs report that TSA uses a document entitled "Medical Guidelines for Transportation Security Screeners" to determine whether a TSO is fit for duty. Has TSA provided the most current version of this document to the American Federation of Government Employees, the union elected as exclusive representative of the TSO workforce?

If not, will you provide the most current version of the Medical Guidelines to the union immediately?

Answer. The current Medical and Psychological Guidelines for Transportation Security Administration (TSA) Transportation Security Officer (TSO) Job Series (TSO Medical Guidelines) have not been provided in their entirety to the American Federation of Government Employees (AFGE), due to the sensitive content contained therein. The TSO Medical Guidelines are intended for use by medical practitioners. Consistent with the 2011 Determination on Transportation Security Officers and Collective Bargaining (2011 Determination) and subsequent 2014 Determination, AFGE did not have the right to the current TSO Medical Guidelines as they do not relate to the issues for collective bargaining. Union representatives who represent individual bargaining unit employees in cases involving the TSO Medical Guidelines

have received, and continue to receive, copies of the relevant section(s) of the TSO Medical Guidelines. TSA is in the process of revising the medical guidelines.

QUESTIONS FROM HONORABLE WILLIAM R. KEATING FOR PETER NEFFENGER

*Question 1a.* Administrator Neffenger: Thank you for your testimony and thoughtful responses at the Transportation Security Subcommittee hearing on October 8, 2015. During our discussion, you said you are conducting a “top-to-bottom” review of all airports, including access control points and what, exactly, constitutes an airport’s perimeter.

What, specifically, has this review entailed and when will it be completed?

*Question 1b.* Once completed, will you provide its findings to interested Members?

Answer. The Transportation Security Administration (TSA) has worked with Federalized airports to closely review all aspects of physical security, including access control points and perimeter security. In doing so, the total number of access points has been reduced by almost 10 percent Nation-wide, while airport security personnel and TSA have increased random screening of airport employees at those access points.

The perimeter security of an airport involves perimeter access and transition areas at the airport, and includes protection of the fence line, active and inactive vehicle & pedestrian gates, maintenance & construction gates, vehicle roadways, and general aviation areas. Access control security generally refers to security features that control who can access certain restricted areas or systems at the airport. At an airport, restricted areas may include the baggage claim area, baggage makeup area, sterile area, secured area, air operations area, catering facilities, cargo facilities, fuel farms, and other public spaces and areas. In the context of access control security at the airport perimeter (for example, direct entry into the secured area through a vehicle access gate), this definition does not include access at a passenger checkpoint.

TSA is working with the Aviation Security Advisory Committee (ASAC) on a comprehensive review of airport perimeter security. ASAC has provided a list of recommendations to improve perimeter security. These recommendations are under review.

TSA will be pleased to share its findings with the committee and interested Members.

*Question 2.* Second, you are aware of my long-standing concern for transitioning the responsibility of staffing airport exit lanes from TSA to airport operators. I have spoken with numerous operators, include the Massachusetts Port Authority (Massport), which owns and operates three airports in Massachusetts, including Boston Logan International Airport, in addition to the Port of Boston. They remain troubled that TSA interpreted the staffing of exit lanes as an issue of access control rather than screening function, and that the expectation for airport operators to staff these exit ways will continue. This is a matter of both safety and resources.

What is TSA’s current policy for staffing exit lanes? Will TSA continue to staff airport exit lanes into the future? If not, how will TSA work with airports to mitigate costs?

Answer. Currently, approximately two-thirds of the airport operators control access at exit lanes by using airport technology or personnel. The remaining exit lanes are staffed by the Transportation Security Administration (TSA). Under § 603 of the Bipartisan Budget Act of 2013 (Budget Act), Pub. L. No. 113–67, Div. A, § 603, 127 Stat. 1188 (2013), TSA is responsible for monitoring passenger exit lanes from the sterile area of airports at which TSA provided such monitoring as of December 1, 2013. TSA interprets § 603 of the Budget Act to mean that TSA must staff a sterile area exit lane only if the exit lane was in existence on December 1, 2013, at one of the 155 airports at which TSA was providing monitoring services on that date. Therefore, if an airport is remodeling an exit lane and the location of this exit remains essentially the same, TSA will continue to staff this lane. If the remodeling significantly changes the location of the exit lane, to where it is no longer co-located with the screening checkpoint, and/or requires additional staffing and resources, TSA is no longer obligated to monitor this exit lane.

TSA provides an evaluation tool, which allows the airport operator to input exit lane configurations and parameters, and receive recommendations for technological solutions. Consideration of technology options to exit lane staffing should also include evaluation of related advantages, disadvantages, and trade-offs in breach response requirements.



## QUESTIONS FROM CHAIRMAN JOHN KATKO FOR JOHN ROTH

*Question 1.* Inspector General Roth, your office has conducted numerous investigations highlighting various challenges that the Transportation Security Administration (TSA) faces. What systemic problems have you identified?

Answer. In the past year, I have testified before your committee and others on my concerns about TSA's enormous and complex challenges. These challenges are systemic; they impact virtually every area of TSA operations. Our audits and reviews have shown that TSA's challenges include:

- assessing risk appropriately;
- contracting for goods and services;
- deploying and maintaining equipment;
- hiring and training an effective workforce;
- performing basic management functions to meet its mission; and
- operating in a culture resistant to oversight and unwilling to accept the need for change in the face of an evolving and serious threat.

*Question 2.* From your perspective what steps do you feel Administrator Neffenger should take to reform and improve TSA?

Answer. Addressing the aforementioned challenges will require time, resources, and committed, courageous leadership at every level of management and throughout the organization, from the TSA Administrator to Transportation Security Officers (TSO) who screen passengers and baggage. Examples of steps TSA should take to reform and improve its performance include:

- Ensure proper staffing, training, and supervision of TSOs to mitigate the effects of human error-related vulnerabilities in passenger and baggage screening.
- Ensure everyone in the chain-of-command understands and is committed to addressing passenger and baggage screening vulnerabilities identified in our reports.
- Encourage all TSA personnel to identify and report security deficiencies and vulnerabilities and participate in developing and implementing solutions.
- Improve the transparency and accountability of efforts undertaken or planned to address the technological, personnel, and procedural deficiencies and vulnerabilities identified by OIG, the Government Accountability Office (GAO), and internal offices, such as TSA's Office of Inspections.
- Implement timely, efficient, and effective strategies to ensure all screening equipment is well-maintained and fully operational.

OIG will continue its oversight of TSA. For example, we plan to:

- determine whether the Federal Air Marshal Service (FAMS) adequately manages its resources to detect, deter, and defeat threats to the civil aviation system (Federal Air Marshal Service Oversight of Civil Aviation Security); and
- determine the effectiveness of TSA's carry-on baggage screening technologies and checkpoint screener performance in identifying and resolving potential threats at airport security checkpoints (TSA Carry-On Baggage Penetration Testing).

Our on-going audits and reviews of TSA include:

- *Office of Human Capital Contracts.*—Determine whether TSA's human capital contracts are managed effectively, comply with DHS's acquisition guidelines, and are achieving expected goals.
- *Security Vetting of Passenger Rail Reservation Systems.*—Determine the extent to which TSA has policies, processes, and oversight measures to improve security at the National Railroad Passenger Corporation (AMTRAK).
- *Controls Over Access Media Badges.*—Identify and test selected controls over access media badges issued by airport operators.

*Question 3.* Looking at your office's extensive body of work as it relates to TSA's technology challenges, stepping back, how can TSA improve its technology procurement and development processes in order to prevent itself from investing in technology that does not adequately meet the current threat environment?

Answer. Our office has also audited and reported on TSA's acquisition programs. Although TSA has spent billions on aviation security technology, our testing of certain systems revealed no resulting improvement. Given the number, type, complexity, and cost of these passenger screening technologies, TSA must exercise due diligence in developing, procuring, and deploying these valuable and costly assets. These systems include:

- Explosives Detection System (EDS) machines
- Explosives Trace Detection machines
- Advanced Imaging Technology (AIT) machines
- Bottled Liquid Scanners
- X-ray machines

- Walkthrough metal detectors.

OIG has conducted a number of audits that identified issues with TSA's procurement, deployment, and maintenance of its passenger screening technologies. These audits raise serious questions regarding TSA's management of its passenger screening technologies. For example, in fiscal year 2013, we reviewed TSA's deployment of AIT machines upgraded with automatic target recognition (ATR) software, an upgrade that addressed privacy concerns raised by travelers and Members of Congress. These concerns led to the passage of the *FAA Modernization and Reform Act of 2012*, which mandated that all AIT screening equipment at airports include the ATR upgrade no later than June 1, 2013.

We determined that TSA failed to develop a strategic acquisition and deployment plan for the AIT machines with the required AIT software that aligned with the overall needs and goals of its passenger screening program. As a result, TSA did not deploy many of the newly purchased or upgraded AIT machines and fully utilize them for screening passengers. This led to continued use of less capable walk-through metal detectors. We made two recommendations to improve future deployment and use of AIT machines.

*Question 4.* A report issued by your office in May found that TSA's airport screening equipment is not being properly maintained. Lack of maintenance not only puts into question the effectiveness of the equipment, but can reduce the life span of technologies, requiring their replacement at the expense of significant taxpayer dollars. What has the TSA done to date, to implement the recommendations of this report?

Answer. In May 2015, we reported that because TSA did not ensure routine preventive and corrective maintenance was performed according to contractual requirements, it could not be certain screening equipment was repaired and ready for operational use. We made three recommendations to improve TSA's oversight of its maintenance program.

We recommended that TSA assess penalties when contractors do not perform preventive or corrective maintenance according to contractual requirements and manufacturers' specifications. We believe TSA's actions are sufficient to close this recommendation. Specifically, TSA recently signed contracts with Morpho Detection and L-3 Communications for preventive and corrective maintenance on EDS equipment. Both contracts include specific financial penalties for maintenance not completed according to contractual requirements. For preventive maintenance, TSA will assess a penalty of 50 percent of the monthly invoice amount for the particular machine. The contracts also include penalty clauses for corrective maintenance actions when they affect operational availability at the equipment and airport level.

TSA has taken steps to implement the other two recommendations, but we do not believe their actions are sufficient to close them. Basically, we recommended that TSA airport personnel validate data on both types of maintenance to ensure that preventive maintenance is completed according to contract requirements and manufacturers' specifications and to ensure its screening equipment is repaired and ready for operational use.

TSA has implemented additional reporting requirements for maintenance contractors that should provide airports with better awareness of maintenance actions on their screening equipment. For example, contractors are now required to give monthly preventive maintenance schedules to airport coordination centers. However, TSA has not yet developed and implemented policies and procedures to verify and document the contractors' completion of all required preventive and corrective maintenance actions. According to TSA, an independent contractor compares the preventive maintenance data with contractual requirements, but this is not the same as validating that the work has actually been performed, which is the intent of our recommendation. Further, although contractors are required to provide certain reports on corrective maintenance, TSA does not have policies or procedures to verify the information in these reports or test the data for accuracy.

*Question 5.* In response to the highly disappointing results of the OIG's covert testing of airport screening procedures, Secretary Johnson mandated that all airport screeners and managers undergo an 8-hour training course. Do you believe that this training is sufficient to address the security gap found in the covert testing? What else, if anything, should be done to ensure that the workforce has the skills they need to effectively perform their duties?

Answer. On September 22, 2015, my office provided TSA with our Classified final report, *Covert Testing of TSA's Passenger Screening Technologies and Processes at Airport Security Checkpoints*, OIG-15-150. TSA has 90 days following receipt of the final report to update us on the status of its implementation of our recommendation. We cannot comment on TSA's training because we have not yet received a formal,

detailed update. The detailed information on TSA's training will most likely contain Classified or Sensitive Security Information and we will not be able to discuss or comment on the content of the TSA training in the public record. However, once we receive the formal update, we would be happy to arrange a meeting with you or your staff to discuss the specific details in a Classified setting.

With respect to other actions TSA can take to ensure its workforce has the skills needed to effectively screen passengers at airport checkpoints, TSA and OIG must continue to conduct covert testing of technology, human performance, and screening procedures used at checkpoints. These covert tests must be continuously updated, based on intelligence about security threats. Rigorous covert testing will help ensure that the TSA workforce is prepared to deal with the constantly-changing threat environment.

*Question 6.* The TSA PreCheck initiative has resulted in more risk-based and efficient screening of passengers at airports. However, a January OIG report found that modifications to the screening and vetting process are necessary. Do you feel TSA has taken the necessary steps to address these concerns?

*Answer.* We reported in January 2015 that TSA's implementation of PreCheck and the expedited screening process increased throughput at airport checkpoints, but also increased the risk to aviation security because TSA was not making individualized risk-based decisions. We made recommendations to address identified deficiencies. Initially, TSA did not concur with the majority of the 17 recommendations in our report, but we have made significant progress in getting TSA's concurrence and compliance. As of November 2015, we have closed 3 report recommendations; 13 recommendations are open, but resolved, meaning we agree with TSA's planned actions to address the intent of these recommendations. Although one recommendation remains open and unresolved, TSA officials said there has been a significant shift to address this recommendation and TSA is currently drafting a response outlining these changes. We would be happy to update you and your staff on the progress once we have received a formal response from TSA.

*Question 7.* Currently fewer than 5% of travelers participate in TSA PreCheck. Do you believe TSA has put ample emphasis on enrolling more passengers in TSA PreCheck? What additional steps do you feel TSA needs to take in order to expand and enhance the PreCheck program?

*Answer.* Our review did not focus on expanding the TSA PreCheck initiative; GAO conducted a review addressing the expansion.

We are currently reviewing TSA's Risk-Based Strategy to determine the extent to which this strategy informs security and resource decisions to protect the traveling public and the Nation's transportation systems. Our report, which we expect to publish in the spring of 2016, will include a discussion of the PreCheck initiative. We look forward to sharing our findings and recommendations with you.

*Question 8.* Prior to Admiral Neffenger's confirmation as administrator, TSA failed to concur with recommendations in a number of your reports. Are there any outstanding recommendations with which TSA has not concurred and taken some steps to address at this time?

*Answer.* We believe TSA is working in good faith to concur with recommendations with which it previously did not concur and to close open recommendations. For example, although TSA did not initially concur with the majority of our recommendations to correct identified TSA PreCheck deficiencies, it continues to seek closure through the recommendation follow-up and resolution process. TSA recently told us it is reevaluating its position on its open recommendations and for the single unresolved recommendation in that report, we are optimistic that TSA is reconsidering the wisdom of its position.

As we reported in *Audit of Security Controls for DHS Information at John F. Kennedy International Airport* (OIG-15-18), TSA did not perform required security authorizations or privacy reviews on closed-circuit television and surveillance monitoring room technology (i.e., cameras) used to record passenger data and photos. We reported that according to DHS 4300 security policy, the cameras should be considered IT assets and counted as part of DHS's asset inventory. TSA did not concur with our recommendation to address this issue, asserting that DHS 4300 security policy did not apply to the cameras. We are currently working with TSA, the DHS Office of the Chief Information Officer, and the DHS Office of Privacy to resolve this issue.

*Question 9.* It is no secret that employee morale is a significant problem at the TSA, both for screeners and agency employees alike. Your office has a unique perspective in that you are able to talk confidentially with TSA employees. Do you have any insights into the underlying cause of the on-going lack of morale at the agency?

*Answer.* DHS OIG has not done any recent audit or inspection work in this area.

*Question 10.* Airports in Miami and Orlando conduct 100% employee screening, yet the Aviation Security Advisory Committee report concluded that 100% employee screening would be too costly to implement Nation-wide. What changes do you feel need to be implemented in order to improve the screening of airport employees?

Answer. Our office is familiar with the Department's Aviation Security Advisory Committee's report and the immediate actions Secretary Johnson took to increase physical screening of aviation employees. We have not conducted work in the area of employee physical screening, but we believe that unscreened airport workers represent a threat to air transportation security. We recently reviewed aviation employee vetting (*TSA Can Improve Aviation Worker Vetting*, OIG-15-98), and our recommendations from that report were very similar to those in a recent committee report. The Aviation Security Advisory Committee and OIG agree that TSA can strengthen airport employee vetting by:

- updating the list of disqualifying criminal offenses;
- continuously monitoring criminal activity (recurrent employee vetting); and
- maintaining a National database of airport employees whose credentials have been revoked.

*Question 11.* The Air Marshal Association, a professional association for members of the Federal Air Marshal Service (FAMS), advocates shifting the workforce to focus on investigations and anti-terrorism operations as opposed to deploying on flights to deter terrorism and hijacking. Do you think this would be a more effective use of manpower and resources?

Answer. We have not done a large-scale review of FAMS that would allow us to draw across-the-board conclusions about whether its legacy mission and goals are effectively aligned with the current threat environment. This year we will audit FAMS to determine whether it adequately manages its resources to detect, deter, and defeat threats to the civil aviation system.

According to the Department's 2014 Quadrennial Homeland Security Review, the terrorist threat has changed since the attacks of September 11, 2001. In our Fiscal Year 2016 Annual Performance Plan, we discussed the threat of organized radical extremist groups repeatedly seeking to recruit members and export terrorism to the United States. We have also seen domestic "lone offenders" and those inspired by extremist ideologies commit terrorist acts. These threats are difficult to detect. In countering terrorism, DHS focuses on preventing attacks; preventing unauthorized acquisition, importation, movement, or use of chemical, biological, radiological, and nuclear materials and capabilities in the United States; and reducing the vulnerability of critical infrastructure and key resources, essential leadership, and major events to terrorist attacks and other hazards. In the upcoming FAMS audit and other audits focused on preventing terrorism and enhancing security, OIG will seek to determine how efficiently and effectively the Department is working to counter these emerging threats.

