OCTOBER 8, 2015

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

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

ONE HUNDRED FOURTEENTH CONGRESS, FIRST SESSION

HEARING CONTENTS:

MEMBER STATEMENTS:

Rep. John Katko (R-NY) *[view pdf]*
Chairman, Subcommittee on Transportation Security

Rep. Kathleen Rice (D-NY) *pdf unavailable; 51:37 of hearing webcast*
Ranking Member, Subcommittee on Transportation Security

WITNESSES:

Hon. John Roth *[view pdf]*
Inspector General, Office of the Inspector General, U.S. Department of Homeland Security

Hon. Peter Neffenger *[view pdf]*
Administrator, Transportation Security Administration
U.S. Department of Homeland Security

AVAILABLE WEBCAST(S):*

Full Hearing: *https://youtu.be/MfEeO1PUUA8?t=2792*

COMPILED FROM:

https://homeland.house.gov/hearing/reform-and-improvement-assessing-the-path-forward-for-the-transportation-security-administration/

** Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*

HOMELAND SECURITY
COMMITTEE

OPENING STATEMENT
October 8, 2015

MEDIA CONTACTS
Susan Phalen, Matthew Ballard

Statement of Subcommittee Chairman John Katko (R-NY)
Transportation Security Subcommittee
House Homeland Security Committee

Reform and Improvement: Assessing the Path Forward for the Transportation Security Administration

Remarks as Prepared

I would like to welcome everyone to today's hearing. I am pleased to have Inspector General Roth and Administrator Neffenger here today as our distinguished witnesses. The purpose of today's hearing is to examine TSA's challenges and identify what changes TSA needs to make to in order to move forward.

TSA was created out of a tragedy, and was quickly stood up to address major security vulnerabilities that terrorists exploited. However, fourteen 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 one hundred audits identifying major security vulnerabilities and organizational challenges throughout TSA, including the most recent reports that found that TSA's passenger screening was allegedly wrong 96% of the time, and that seventy-three aviation workers had potential ties to terrorism. These figures are startling and shatter public confidence. I look forward to hearing from you today 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, are not isolated instances; many of these vulnerabilities have been identified and known for years, and unfortunately, prior to this year, the previous leadership within both TSA and DHS did not take steps to address these known security vulnerabilities.

However, the purpose of today's hearing is not to look backwards. With new leadership, Administrator Neffenger, you have an opportunity to address these challenges head on, and lead TSA on a different path. In our discussions, you have been frank, straightforward and sincere. I have full confidence that you are tackling TSA's challenges with an open mind, and 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 seven pieces of legislation pass the House, and two 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% of the time and the terrorists only have to be right once.

With nearly two 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% of travelers 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 comprehensively to improve the effectiveness of access controls at airports across the United States. 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 transportations 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 duty to spur action and keep the traveling public safe from harm. Inspector General Roth and Administrator Neffenger, this committee wants to support both of you in your efforts to reform TSA, and we look forward to hearing from you today.

###

STATEMENT OF JOHN ROTH

INSPECTOR GENERAL

DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

HOUSE COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON TRANSPORTATION SECURITY

U.S. HOUSE OF REPRESENTATIVES

CONCERNING

Reform & Improvement: Assessing the Path Forward for the Transportation Security Administration

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 eight 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 onboard 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 11th 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 two 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 onboard 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.[1] 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

[1] 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.

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 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 FYs 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 applicants' 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 one 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

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-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 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 Sensitive Security Information.	Closed	Agreed

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-12-06	Transportation Security Administration Penetration Testing of Advanced Imaging Technology	11/21/2011	Recommendation includes Sensitive 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 (SPOT) program that includes—Mission, goals, objectives, and a system to measure performance; A training strategy that addresses the goals and objectives of the SPOT 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
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

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-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

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-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
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

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-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 Sensitive Security Information.	Open – Resolved	**Agreed****

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-14-153	Use of Risk Assessment within Secure Flight	9/9/2014	Recommendation includes Sensitive Security Information.	Closed	Agreed
OIG-14-153	Use of Risk Assessment within Secure Flight	9/9/2014	Recommendation includes Sensitive Security Information.	**Closed***	**Agreed****
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Unresolved	Disagreed
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Resolved	Agreed
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Resolved	Agreed
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Resolved	Agreed
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Resolved	**Agreed****
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Resolved	Agreed

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-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	**Open – Resolved***	Agreed
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	**Closed***	**Agreed****
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	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 exclusion factors to refer TSA 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 Sensitive Security Information.	**Closed***	Agreed
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	**Closed***	Agreed

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-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 Sensitive Security Information.	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: 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

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-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

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-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
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 noncompliance 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 six 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' 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.

Statement of Peter Neffenger
Administrator, Transportation Security Administration
U.S. Department of Homeland Security
Before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on Transportation Security
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 transportations 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 FY 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 six million air passengers against the U.S. 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 FY 2014TSA 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 ten-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 nationwide 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 ongoing, 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 12th, 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 two weeks. These updates have been ongoing 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

frontline 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 frontline 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[1] create a stressed screening environment at airport checkpoints. The challenges also include the

[1] 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).

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 resourcing 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.

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 frontline 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 systemically 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 frontline 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 FY16, 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 1st, we have trained the specifics of the failures to virtually every frontline 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 Pre✓® or in other DHS trusted traveler programs. In parallel, 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 six out of eight 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 frontlines 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.