

DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS FOR FISCAL YEAR 2016

TUESDAY, SEPTEMBER 29, 2015

U.S. SENATE,
SUBCOMMITTEE OF THE COMMITTEE ON APPROPRIATIONS,
Washington, DC.

The subcommittee met at 11:20 a.m., in room SD-138, Dirksen Senate Office Building, Hon. John Hoeven (chairman) presiding.
Present: Senators Hoeven, Shaheen, and Baldwin.

DEPARTMENT OF HOMELAND SECURITY

STATEMENTS OF:

HON. JOHN ROTH, INSPECTOR GENERAL

**HON. PETER V. NEFFENGER, ADMINISTRATOR, TRANSPORTATION
SECURITY ADMINISTRATION**

OPENING STATEMENT OF SENATOR JOHN HOEVEN

Senator HOEVEN. The subcommittee will come to order. Good morning. I would like to welcome our witnesses this morning. First, I would like to thank Ranking Member Senator Shaheen for being here and for her work. And then I would like to welcome both Administrator Peter Neffenger as well as the inspector general, John Roth. We appreciate both of you being with us this morning.

This month marks the 14th anniversary since the attacks on 9/11. Our Nation's response to that terrible day's events included significant and immediate investment in aviation security, and billions of dollars were spent on new people, processes, and technology to build layers of security.

These layers start with intelligence programs and passenger pre-screening in advance of travel, and in the plane itself with hardened cockpit doors, and awareness of passengers and crew members. These layers are intended to be adaptive and agile in responding to current threats and tactics. And this is important given our adversaries' continued fascination with aviation as a target and their changing methods.

However, now it appears that the security provided by the most visible and expensive layer, the screening checkpoint itself, has been overestimated. Specifically, media reports cited that the Transportation Security Administration (TSA) has a failure rate of over 90 percent in covert testing of checkpoints. For obvious reasons we cannot elaborate on the details of those tests in an open hearing. However, the failure calls into question the effectiveness

of the people, the training, the processes that we have instituted, and the technology.

And remember, all three have to work. All three legs of the stool—people, process, and technology—have to be strong and balanced to maintain the security system. And clearly we need to review the entire process, all three legs, and make changes to make sure that security is as effective as possible.

With respect to the people, TSA screeners have a challenging job: they must stay focused on their security mission while performing repetitive tasks in a high-pressure, high-throughput environment. Meanwhile, organizations like al Qaeda disseminate inventive ways to smuggle contraband onto airplanes and avoid security measures.

Supporting this workforce must be the right processes. These procedures must be tested and trained as well as applied consistently. Many of these processes, as we are all aware, are uncomfortable both for the screeners and the passengers, and appreciation of both points of view is critical.

Last, TSA has always sought with varying degrees of success to embrace cutting-edge technology. The 2009 Christmas Day plot and the use of non-metallic explosives aboard a commercial aircraft demanded a solution. The advanced imaging technology (AIT) we have deployed is not a silver bullet. All these facts—the people, processes, and the technology—must work in concert. Must work in concert. A failure of any one weakens the entire system.

PREPARED STATEMENT

Today the inspector general issued the final report associated with the leaked testing information. To the extent possible in an open hearing, I have asked the inspector general to lay out the findings and recommendations in that report. He will also outline his office's other work on passenger screening in recent years.

Secretary Johnson responded quickly to the leak back in June outlining a 10-point plan of action. That plan is now yours, Administrator Neffenger's, to shape and to execute. I look forward to questioning you about the plan in detail, including the resource implications, which, of course, is our area of responsibility, and the right metrics by which to measure progress and success. Very important. We have to have a way to measure our progress and success.

[The statement follows:]

PREPARED STATEMENT OF SENATOR JOHN HOEVEN

The Subcommittee will come to order. Good morning. I would first like to welcome our witnesses. Administrator Peter Neffenger is the recently confirmed Assistant Secretary of the Transportation Security Administration. The Coast Guard's loss is TSA's gain and we look forward to working with you in this capacity.

And the Department of Homeland Security's Inspector General, John Roth. Thank you both for being here.

Thank you also to Ranking Member Shaheen and other subcommittee members for your time and attention to this important issue.

This month marks the 14th Anniversary since the attacks on September 11th. Our nation's response to that terrible day's events included a significant and immediate investment in aviation security. Billions of dollars were spent on new people, processes, and technology to build new "layers" of security.

These layers start with intelligence programs and passenger pre-screening in advance of travel and end in the plane itself with hardened cockpit doors and aware passengers and crew members.

These layers are intended to be adaptive and agile, responding to current threats and tactics. This is important given the adversary's continued fascination with aviation as a target.

However, it now appears that the security provided by the most visible—and expensive layer—the screening checkpoint itself, was overestimated. Specifically,

media reports cited that TSA had a failure rate of over 90 percent in covert testing of checkpoints.

For obvious reasons, we cannot elaborate on the details of those tests in an open hearing. However, the failures call into question the effectiveness of: (1) the people we have hired and trained; (2) the processes we have instituted; and (3) the technology we have procured.

All three legs of the stool—people, process, and technology—have to be strong and balanced to maintain the security system. And, it seems to me, that we need to review our entire system and make changes to ensure it is effective.

With respect to people, TSA screeners have a challenging job. They must stay focused on their security mission while performing monotonous tasks in a high pressure, high throughput environment. Meanwhile, organizations like al-Qaeda disseminate inventive ways to smuggle contraband onto airplanes and avoid security measures.

Supporting this workforce must be the right processes. These procedures must be tested and trained as well as applied consistently. Many of these processes—as we’re all aware—are uncomfortable for both the screeners and passengers. An appreciation of both points of view is critical.

Lastly, TSA has always sought—with varying degrees of success—to embrace cutting edge technology. The 2009 Christmas Day plot and the use of non-metallic explosives aboard a commercial aircraft demanded a solution. But the Advanced Imaging Technology we have deployed is not a silver bullet.

All of these facets: the people, the processes, and the technology, must work in concert. A failure of one weakens the entire system.

Today, the Inspector General issued the final report associated with the leaked testing information. To the extent possible in an open hearing, I have asked the Inspector General to lay out the findings and recommendation in that report. He will also outline his office’s other work on passenger screening in recent years.

Secretary Johnson responded quickly to the leak back in June outlining a 10-point plan of action. That plan is now Administrator Neffenger’s to shape and execute. I look forward to questioning him about the plan in detail, including the resource implications and the right metrics by which to measure progress and success.

Senator HOEVEN. With that, I’d turn it over to Senator Shaheen for her opening comments.

STATEMENT OF SENATOR JEANNE SHAHEEN

Senator SHAHEEN. Well, thank you very much, Mr. Chairman, both for your remarks and for calling this hearing this morning. I also want to thank Administrator Neffenger and Inspector General Roth both for being here this morning and for taking on the very challenging jobs that you are doing so well.

The point of the hearing today is really to assure the public that TSA is taking the appropriate steps to make air travel safe and to see that taxpayer dollars for aviation security are being spent wisely. As Chairman Hoeven pointed out, earlier this year the inspector general performed an audit of TSA screening by conducting numerous tests across eight airports of different sizes. The data from the audit are classified, but I think it is fair to say that all of us agree that the results were extremely troubling.

The results from those tests were so concerning that the inspector general halted the audit before it was completed in order to inform the Secretary of Homeland Security that TSA had a major problem. The Secretary responded by putting together a Tiger Team of Department of Homeland Security (DHS) and TSA officials to fully evaluate TSA’s screening apparatus. He also called for agency officials to think outside the box, to challenge old assumptions, and to listen to the Transportation Security Administration offices in the field who are doing the job day in and day out.

So today we will explore what the Tiger Team found, and discuss changes that are being made to screening techniques, to standard

operating procedures, employee training and technology, and other innovative ideas to improve the agency. Now, again, as Chairman Hoeven pointed out, because this is the appropriations subcommittee on Homeland Security, we are very concerned about what the resource implications are if these changes are implemented. We will be looking at TSA's risk-based approaches to passenger screening, and whether there is an appropriate balance between security effectiveness and screening efficiency.

So, again, Mr. Chairman, thank you for holding this hearing today, and I look forward to hearing from our witnesses.

Senator HOEVEN. Thank you, Senator Shaheen. I will also now turn to Senator Baldwin. Thank you for joining us, and ask if you have any opening comments.

Senator BALDWIN. Other than to thank you and the ranking member for holding this hearing. As a member of both the Homeland Security and Governmental Affairs Committee and the Appropriations Subcommittee on Homeland Security, following on implementation of recommendations from the inspector general has been a great concern of mine, and I will have several questions after the testimony is received. But I look forward to hearing that testimony, and thank you for holding this hearing.

Senator HOEVEN. Thank you, Senator Baldwin. With that, I would turn to John Roth, the inspector general, for his report.

SUMMARY STATEMENT OF HON. JOHN ROTH

Mr. ROTH. Good morning, Chairman Hoeven, Ranking Member Shaheen, and members of the subcommittee. Thank you for inviting me here to testify regarding our work involving TSA. Our reviews, and there have been 115 reviews, audits, and inspections, that have given us a perspective on the obstacles facing TSA in carrying out its important, but very difficult, mission: to protect the Nation's transportation systems while at the same time ensuring freedom of movement.

I have been deeply concerned about the challenges TSA faces in their ability to meet those challenges. These challenges are in almost every area of TSA's operations: its problematic implementation of risk assessment rules, including the management of TSA PreCheck; deficiencies in TSA's duties as a regulator of our Nation's 450 commercial airports, particularly in the area of employee screening; failures in passenger and baggage screening operations, discovered in part for a covert testing program; TSA's controls over access to secure areas, including management of its access badge program, its management of its workforce integrity program, and its oversight over its acquisition and maintenance of screening equipment.

I will confess to a degree of frustration that TSA was assessing risk inappropriately and did not have the ability to perform the basic management functions it needed in order to perform this crucial mission. These issues were exacerbated, in my judgment, by a culture that resisted oversight and was unwilling to accept the need for change in the face of an evolving and serious threat. We had been writing reports highlighting some of these reports for years without an acknowledgement by TSA of the need to correct those deficiencies.

However, we may be in a very different place than we were in recent months. I am hopeful that Administrator Neffenger brings with him a new attitude about oversight. It will take a sustained and disciplined effort, but having the courage to critically assess these deficiencies in an honest, objective light is the first step, and I believe TSA has taken that first step in recent months.

We have just completed and distributed our report on our most recent round of covert testing. The results, of course, are classified at the secret level, and the Department and this committee have been provided a copy. The testing, as the chairman points out, was of the AIT equipment, the advanced imaging technology, in use at airports across the country. This is the state-of-art in imaging technology.

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 our auditors 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. The results were consistent across every airport.

Our testing was designed to test checkpoint operations in real world conditions. They were not designed to test specific discreet segments of checkpoint operations, but rather the system as a whole. The failures included failures in technology, in TSA procedures and process, 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 in the totality of aviation security.

The results unfortunately were not unexpected. We had conducted other covert tests in the past of check baggage X-ray screening, of access controls to secure airport areas, of the screening of carry-on luggage, and of the previous generation of AIT machines that were in use several years ago. In each of these tests, we discovered significant vulnerabilities.

Fortunately, the Department's response to our most recent findings has been swift and unequivocal. For example, within 24 hours of receiving the preliminary results of the Office of the Inspector General (OIG) covert testing, the Secretary summoned TSA leadership and directed that an immediate plan of action be created to correct the deficiencies uncovered by this testing. These efforts have already resulted in significant changes to TSA leadership, operations, training, and policy.

TSA has put forward a plan consistent with our recommendations to improve checkpoint quality in three areas: technology, personnel, and procedures. This is appropriate, as the chairman noted, 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 appropriate procedures. Unless all three elements are operating effectively, the checkpoint itself will not be effective. However, this is a difficult problem, and it will take time to fix.

PREPARED STATEMENT

We will be monitoring TSA's efforts to increase the effectiveness of checkpoint operations, and we 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.

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

[The statement follows:]

PREPARED STATEMENT OF HON. JOHN ROTH

DISCUSSING THE TRANSPORTATION SECURITY ADMINISTRATION'S EFFORTS TO ADDRESS
INSPECTOR GENERAL FINDINGS

Good morning Chairman Hoeven, Ranking Member Shaheen, and Members of the Subcommittee. Thank you for inviting me here today to discuss our work on the Transportation Security Administration (TSA) and areas we believe are in need of attention for improving the agency. 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.

I testified before a different Congressional committee in May of this year regarding my concerns about TSA's ability to execute its important mission. At that hearing, 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 by a Senator at Administrator Neffenger's confirmation hearing 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 com-

parison 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. They were not designed to test specific, discrete segments of checkpoint operations, but rather the system as a whole. The failures included failures in the technology, in TSA procedures, and in 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 this round of 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 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.

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—with TSA 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 with no formal ties to the larger organizations but 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 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 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.

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.

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. We are doing work currently in this area as well, 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 pro-

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.

gram 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, the program remains an example of a questionable investment in security.

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 looking at 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 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.

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

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
OIG-12-06	Transportation Security Administration Penetration Testing of Advanced Imaging Technology.	11/21/2011	Recommendation includes Sensitive Security Information..	Closed*	Agreed

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
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

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
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

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-13-20	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
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**
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

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..	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..	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
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

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: 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

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 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 RailReservation Systems	Determine the extent to which TSA has policies, processes, and oversight measures to improve security at the National Railroad Passenger Corporation (AM-TRAK).
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 IntegratedProgram (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 I11Risk-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.

Project Topic	Objective
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.

Senator HOEVEN. Thank you, Mr. Roth, and at this point I would turn to Administrator Neffenger.

SUMMARY STATEMENT OF HON. PETER V. NEFFENGER

Mr. NEFFENGER. Thank you. Good morning, Chairman Hoeven, Ranking Member Shaheen, members of the subcommittee. Thank you for the opportunity to testify today and to tell you of our response to the recent challenges that Inspector General Roth has highlighted.

TSA at its core is a counterterrorism organization, an instrument of national power to deter and detect threats and to protect legitimate trade and travel. We have a no fail mission to protect our transportation system. This is a mission for which the consequences of a successful attack overwhelm the risk equation, and for which we must ensure we deliver success. This critically important core mission is my highest priority, and I will tell you that I was greatly disturbed by the inspector general's findings, which came to light during my confirmation process.

As I appear before you today, I am in the middle of my third month on the job. In that 3-month period, I have traveled extensively to airports and Federal Air Marshal Service offices across the country. I even managed to get over and visit with a few of my counterparts in Europe. And I have been thoroughly impressed with our professionals who occupy our ranks, our officers, our air marshals, inspectors, and other employees who swore an oath to serve their Nation in a mission that encounters nearly 2 million travelers per day in the aviation sector alone. I have had time to become more familiar with the challenges facing the agency and to develop a series of immediate priorities. One of those is to pursue solutions to the recent covert testing failures.

Overall, there are several critical elements that are essential to improving screening operations. First, we must ensure the appropriate measures of effectiveness are in place to drive an institutional focus on our primary mission. What we measure is what our employees will pay attention to, so it is imperative that we get our measures correct. Second, we must employ a culture of operational evolution, one that constantly reassesses assumptions, plans, and processes, and it must be able to rapidly field new concepts of operation. And finally, we must deliver an effective system and earn the confidence of the traveling public, and this will only come through competence, discipline, performance, and professionalism.

I have conveyed these standards to our workforce, and I commit to you that I will relentlessly pursue these objectives.

We continue to face an adversary intent on attacking the transportation sector, an adversary who is adaptive and patient, who presents threats that are complex, decentralized, and evolving, and these are TSA's most pressing challenges. They require a renewed focus on our security mission. We face a critical turning point in evolving TSA, both to address the findings of the inspector general's report and to begin our investment in security technologies that can propel us into the future.

Aviation security includes a range of capabilities, some seen, many unseen, and every day we employ invaluable tools. Our intelligence experts, passenger screening canines, behavioral detection, Federal air marshals, and many others that protect the transportation system that as recent and prior tests show, we must continue to improve our effectiveness in checkpoint screening, which is the fundamental element of the passenger screening process.

I want to thank Inspector General Roth for his review. I met with him prior to my nomination, and I met with him as the administrator to relay the seriousness with which I take his work, and to gain his continued insights. My staff has met with his inspection team multiple times following his screening assessment, and his team has been invaluable in helping us to identify root causes.

So in response to these findings, TSA implemented an immediate action plan. The plan ensures leadership accountability, improves alarm resolution, increases effectiveness and deterrence, increases threat testing, and strengthens procedures.

We have also responded vigorously to Secretary Johnson's 10-point plan to review and assess screening operations, including mission-sensitive training for the entire screening workforce, which occurred over the past 2 months. We will complete that as of the end of this week. Testing and improving the technology, and implementing new procedures and explosion detection capabilities. We continue to implement this plan of action, and we will continue to provide regular updates to the Secretary and to our oversight committees in the Congress.

Of the utmost concern is determining the root causes for the failures noted. Our conclusion is that the screening effectiveness challenges were not merely a performance problem, not merely a process problem, nor were they a failure principally of the advanced imaging technology. Indeed, AITs have greatly enhanced our ability to detect non-metallic threats, and they continue to perform to expected standards when used properly.

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

Our analysis also revealed that our officers did not fully understand the capabilities and limitations of the equipment that they were using, and several procedures were inadequate to resolve

alarms. We have addressed these, and we have trained our officers to understand and to use the equipment properly.

Solutions to these challenges require a renewed focus on security; more streamlined, more effective procedures; investments in technology; realistic and standardized training, and new balance between effectiveness and efficiency, and support for our frontline officers. We will continue to partner with the airlines and with airport operators in the trade industry to identify solutions that can reduce the stress on the checkpoint, and we must rightsize and resource TSA appropriately.

Our near-term solutions will halt further reductions in officer staffing to support screening operations; provide consistent, high-quality training at a centralized location; and enhance our technology at checkpoints. With your support we can fund the majority of these investments using base resources.

As noted, a key element of our solution is to halt further reductions in our frontline screening workforce. Staffing levels for fiscal year 2016 planned nearly 2 years ago presumed a significant increase in the vetted traveling population, PreCheck passengers, which, combined with the practice referred to as management inclusion, could have allowed for a smaller screening workforce.

Budgeting assumptions for fiscal year 2016 also predated the rise of ISIL (Islamic State of Iraq and the Levant) and the renewed transportation security threats we face today. Thus, I am asking that we hold staffing at current levels as of summer 2015, which is about 5,600 below where we were in 2011, and includes fiscal year 2016 reductions that have already been taken in certain aspects of our workforce.

Our mission-essentials training conducted the past 2 months with every frontline officer and leader across TSA has helped to reset our focus on security effectiveness, and most critically we have enhanced our officers' knowledge of the screening systems they employ. And I have met with our officers in airports across the country and attended the training sessions myself. I have heard repeatedly how valuable this information is to them.

Our new officer training across the country requires greater consistency and efficiency in its delivery, and we must do more to establish the 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 (FLETC) in Glynco, Georgia, and plan to send, if approved, all new hire transportation security officers (TSOs) to TSO basic training beginning in January 2016. Centralized training in a formal, professional academy ensures consistency and professionalism, and produces greater enthusiasm, increased confidence in one's skills, dedication, and connectedness to a common agency culture and increased focus on mission. The Senate mark, when added to existing base resources, would fund this training.

We have two existing business case analyses. They were performed in 2008 and 2011. My staff is updating those at this moment. I will provide both of those to you and your staff once we have completed that task. And we have hosted eight prototype courses this past year at FLETC to validate the concept.

I am deeply committed to this effort because I have seen the value a common foundation of training, culture, and operational focus can have on a distributed workforce during my 34 years in the United States Coast Guard. This initiative will improve our mission focus, and we expect it will increase our ability to retain and lead a more highly motivated and mission-ready workforce.

Finally, we are asking for funding for critical AIT technology software and hardware upgrades. These investments are essential to our effectiveness, which I would be pleased to discuss in detail in a classified setting.

[The statement follow:]

PREPARED STATEMENT OF HON. PETER NEFFENGER

Good morning Chairman Hoeven, Ranking Member Shaheen, and distinguished members of the Subcommittee. Thank you for the opportunity to testify in my new role as Administrator of 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 the checkpoint of the future.

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 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 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, high-

lighting 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. Last week I also 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. TSA is now implementing this training in a phased approach, which began May 29, 2015 and is to be completed by the end of September 2015. Over 98 percent of our workforce had completed training as of this hearing.

- 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 was phased out of 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 for the past 2 months.

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 efficiency and speed in screening operations rather than security effectiveness. These challenges range across six dimensions: leadership, technology, workforce performance, the environment, operating procedures, and system design. Of these six, strong drivers include leadership focus, environmental influences, 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) standard¹ 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, creating pressures to expand the populations receiving expedited screening in TSA Pre-Check lanes, even if they had not enrolled in the program, 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.

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.

¹The 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).

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 the end of 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. The field has been notified of the new performance expectations and officer performance plans will be in place by October 30th, 2015, using these new standards.

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 and establishing the new funding baseline for the screening workforce. Prior 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 recommend to the Committee that we hold staffing at fiscal year 2015 levels—with additional adjustments to support training and operational enhancements—to ensure future reductions remain rational choices that balance effectiveness with efficiency. We recognize that this additional personnel request may require additional funding, and look forward to working with the Subcommittee to identify resources to meet these emergent requirements. 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 fiscal year 2016 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, requiring authority and funds in fiscal year 2016/2017 to support our efforts.

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. By the end of this September, we will have trained the specifics of the failures to 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. As of September 29, over 98 percent of the TSO workforce had completed the training. 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 been exposed to this information before. 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 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 “boardingpasses” 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 all 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 Hoeven, Ranking Member Shaheen, 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.

DHS OIG HIGHLIGHTS

COVERT TESTING OF THE TRANSPORTATION SECURITY ADMINISTRATION'S PASSENGER SCREENING TECHNOLOGIES AND PROCESSES AT AIRPORT SECURITY CHECKPOINTS

UNCLASSIFIED SUMMARY

The Transportation Security Administration (TSA) conducts or oversees passenger checkpoint screening at 450 Federalized airports. Passenger checkpoint screening is a process by which passengers are inspected to deter, detect, and prevent explosives, incendiaries, weapons, or other security threats from entering sterile areas of an airport or getting onboard an aircraft.

As threats to transportation security evolved, TSA needed a screening technology to detect nonmetallic threats. TSA developed Advanced Imaging Technology (AIT) to screen passengers for both metallic and nonmetallic threats concealed under clothing—without physical contact. In 2013, TSA equipped all AIT with Automated Target Recognition software, which displays a box around anomalies on a generic outline of a body.

Our objective was to determine the effectiveness of TSA's AIT, Automated Target Recognition software, and checkpoint screener performance in identifying and resolving anomalies and potential security threats at airport checkpoints. The compilation of the number of tests conducted, names of the test airports, and quantitative and qualitative results of our testing is classified or designated as Sensitive Security Information. We have shared the information with the Department, TSA, and appropriate Congressional committees.

We made one recommendation that when implemented should strengthen the effectiveness of identifying and resolving security threats at airport checkpoints.

10-POINT SCREENING OPERATIONS PLAN

Senator HOEVEN. Thank you, Administrator Neffenger. Thank you, Inspector Roth. We will now go to questions and responses in 5-minute rounds.

And I would like to start with you, Administrator. Pursuant to the 10-point plan that the Secretary put forward in June—and you touched on some of this in your opening comments—has the training been completed? Have you put everybody through the training? Have you completed updating the operating procedures, and have you engaged all of the technology vendors on the equipment failures? And the second part is, how are you measuring performance—back to the metrics—and whether you have achieved the level of performance that you need both in terms of safety and in terms of trying to be as convenient as possible for the traveling public?

I know it is kind of a lot, but, again, three legs of the stool: specific progress on each one, and how you are measuring that both in terms of safety and convenience to the customer?

Mr. NEFFENGER. Well, thanks, Mr. Chairman, for the question, so let me address each one. So this is the people, process, and technology pieces, and I will address each one in order.

So with the people piece, we will this week complete the training of our entire frontline workforce. The latest numbers I got the latest this morning, we were at about 98 percent, and that is of the

41,000-plus screeners that we have, they have all been through what we call mission essentials training. That is an eight-hour block of time specifically dedicated to looking at not just the nature of the failures, but then what we do about correcting, by training, those failures.

So that is looking at the actual specific things that were done by the inspector general's team, you know, what items got through, what was the nature in which they got through, and how were they presented at the checkpoints when they went through.

The second piece of that was there is—concurrent with the training—an update on the current threat situation to refocus people on the mission and then to look at what we need to change in order to make sure that does not happen again. So what were the root causes of that? Some of it—and, again, without getting into classified details—has to do with how you present yourself in the equipment, how the equipment is used, and understanding what the equipment can do and what it cannot do.

So that was the purpose of that 8-hour mission essentials training, and, again, everybody has been through that. I also required all of the managers to go through that as well, including the Federal security directors (FSDs) because I did not want this just to be focused on the workforce. The management of that workforce has to understand as well what those issues were. I will talk about the testing of all that in a moment.

The process piece. I looked at the standard operating procedures that we have, and I will tell you I was shocked to see how thick these were. So there were some 3,100 separate items that we expect that a frontline screening workforce officer, a transportation security officer to memorize and to remember. That is an impossibility, and I would argue, not necessary to meet the mission. So one of the things that we have done over the past 6 months is to dramatically streamline those procedures to turn them into more of a quick guide, a response guide. So we have taken that huge, thick binder and turned it into a small binder of operations. I'm happy to share that with the committee so that you can see what the changes are from what we had then to what we have now. And then train to those procedures so that it becomes a very clear and straightforward process to follow.

We have also looked at the way in which we required certain actions to take place to resolve alarms. And what we found was that for the same type of alarm, we sometimes had multiple different processes that we expected people to follow to do that. Well, that is just hard to follow, and it is hard to remember, and it allows gaps and vulnerabilities to exist.

We looked at standardizing the way we resolve alarms, including when you conduct a pat-down. What is that you are doing? What is the purpose of the pat-down? What do we expect to find, and what does it mean to actually resolve an alarm and not simply go through the motions of resolving the alarm?

To test all of this, you have got to go back and see whether or not you have made any progress, and I have talked to Inspector General Roth about the follow-on testing that they are doing. We are doing some follow-on testing ourselves. We are increasing the rate, type, and detail of our own internal covert testing, providing

more immediate feedback, and then doing an immediate measured assessment of performance so that we have a baseline. So we take some of this as a baseline, and then we establish a baseline going forward.

With respect to the technology, I met personally with the leadership of the technology manufacturers—the primary technology manufacturers, including the manufacturer of the AIT machine. They assured me of their commitment to solving some of the software challenges. They are working hard on that right now. We are working with them. We are holding them to account. We are looking forward to some software upgrades that we are testing right now. Initial tests are promising. We have to now put those into an operational field environment to see how well they work. We are also looking at the potential over the coming year to do hardware upgrades, which would increase the resolution of the machines that we are currently using.

Again, how we measure that is we have got to go back and test it, so there is a tactical measure that has to be done we immediately go back and see whether or not devices are able to be moved through the checkpoint in a way that they were before.

I believe that we can—that through a combination of training of our people, understanding, you know, how far the technology can take you, how does the human piece fill that technology gap that will always exist, and then what are the processes to streamline them and make them as straightforward and as consistent as possible across the enterprise. Then we can begin to measure the performance of the system against those.

Senator HOEVEN. Senator Shaheen.

Senator SHAHEEN. Thank you. Mr. Roth, I just want to clarify a couple of things that you said in your testimony. I think I understood you to say that you have done 115 reviews through the inspector general's office of TSA. I assume that has been since the organization or that agency was formed?

Mr. ROTH. That is correct.

Senator SHAHEEN. And you also alluded to a very different response in—to this audit from some of the previous audits. And can you just again make that comparison because I think that is really important for the traveling public to hear. And, again, to point out, as Administrator Neffenger did, to some extent that he was actually not at the head of the organization when the audit was done.

Mr. ROTH. That is exactly right. As you noted in your opening statement, we actually cut the audit off before its planned completion because of some of the results. And I was able to personally brief the Secretary and the chief of staff on that really within a day or two of us conducting the last audit and making the decision that this had to be reported up immediately. We could not wait for the draft. You know, what we would do is we would write a draft, and there would be a formal comment, and then it would come back.

Literally within 24 hours, there was a meeting with the senior leadership at TSA with the Secretary and the Deputy Secretary asking some very serious and pointed questions as to what was going on. And I was able to brief my auditors on it, some of whom had been here since TSA started, and they had never seen any-

thing like it. The response was immediate, it was unequivocal, and it was highly gratifying, at least from our point of view.

AVIATION SYSTEM SECURITY: WORKING WITH OTHER PLAYERS

Senator SHAHEEN. Thank you very much. Administrator Neffenger, you talked a little bit about the people, process, and technology as the chairman did, and about efforts to address all three of those. But as we know, TSA is not the only actor when it comes to keeping our transportation systems secure. So what are you looking at with respect to airports, and air carriers, and the other players in making sure we have a secure environment?

Mr. NEFFENGER. Well, thank you, Senator, and you are absolutely right. You have to look at the entire system. TSA is one component of a very large and complex system that is the aviation environment. So if we are just talking about the aviation sector, there are lots of opportunities for threats to enter into that system whether you are talking the passenger environment, or the aviation—the operating area environment, or the various actors in that environment.

So the first thing I have done is I have actually met with quite a few of the various players and their representatives. So I have met with Airports Council International. They represent the airports. I have met with a number of airport directors in my visits. So I have tried—when I visit an airport, I make it a point to meet with the airport director as well.

I met with the Aviation Security Advisory Committee which, as you know, was asked by the Secretary earlier this year to take a hard look at the trusted work environment as a result of some of the challenges that were raised by the operation in Atlanta that was uncovered, the smuggling that was uncovered.

Just this morning, in fact, before this hearing, I met with the CEOs of all of the major U.S. airlines along with the CEOs of the major cargo airlines to specifically discuss collaborating and understanding their role in the security of the aviation system. No government agency by itself is going to secure this transportation system. You have to have the assistance, the cooperation, and the commitment on the part of all the other players.

I will assure you that that commitment and desire to collaborate and cooperate is there. I think that in TSA, there are—there are lots of places we could continue to improve that relationship and to work more closely with the private sector. There is nobody with a greater vested interest in the security of this system than the people who are operating the system: the airlines, the airports, and all the rest.

So my commitment to them has been to work with them very closely, to look for opportunities to advance our security systems, to look for creative and innovative approaches, to get their help in understanding the system better, to find out where we are working well together and where we are not working well together.

So, as I said, as I get smarter in this, I intend to stay very connected to the industry that we regulate, that we oversee, and that we operate within to ensure that we are an effective partner in that in addition to being good at what our primary mission is.

AVIATION SYSTEM SECURITY: OVERSIGHT

Senator SHAHEEN. And so, TSA has a coordination role in addressing those kinds of issues, and I agree with you. I think the private carriers, the airports, everybody has a stake in making sure the system is as safe as possible. But I also appreciate that sometimes players may not act always with that in mind.

And so, what kind of responsibility does TSA have when you see something that is not being done in a way that you think is proper and particularly safe? What can you do, and do you have statutory responsibility?

Mr. NEFFENGER. We have statutory oversight responsibility for the security of the aviation system. And, again, I will focus on the aviation system, but much of the attention is for the surface transportation world as well.

As I look at the aviation system, certainly, I think what an agency like ours can do best is to ensure a high set of standards, that those standards are enforced consistently across the system, and that there is a regular oversight of the implementation of those standards, even if we are relying upon the private sector to implement and manage those.

I take my experience. When I look back to my experience in the maritime sector as a Coast Guard officer, I spent much of the latter part of my career in the maritime security world. Again, it is a bigger world than there are people in the government to oversee it. I think that is okay as long as you have got strong and consistent standards and a good oversight program there. I think we need to pay attention to that oversight rule more consistently, I think, when you look at things like the trusted worker population that is the badged population.

It never surprises me to find out we have a criminal element in society. It concerns me if we are not doing something to identify that criminal element and to wrest it out of the environment where we think it could pose the greatest challenge and the greatest problem.

So I am encouraged by the report that the Aviation Security Advisory Committee (ASAC) provided, which recommended methods for reducing the number of access points, for example, to the sterile and secure areas of the airport environment, to do more effective randomized routine screening of people who have badges. We are working with the FBI to implement what is called Rap Back, which is a real-time continuous assessment of people's criminal history. We do a real-time assessment of their potential connection to known or suspected terrorists, but we do not currently do that for criminal history. We are doing that on a 2-year basis, so we are piloting some projects with them.

I think that there is more we can do in that environment, and as I look at the recommendations that came out of the Aviation Security Advisory Committee, there were 28 in total, many of them focused directly on this issue you are talking about. We are working on a plan to implement those so that you do not just receive these recommendations and go, thank you very much, and move on. It is very tempting to do that if you are not careful.

So what I want to do is avoid that temptation, and I have gone back to the ASAC and said, look, I promise you to come forward with next steps, and I will do the same thing for oversight committees. You hold yourself accountable by making yourself accountable to the people that are asking the questions. As I said, as I look forward, I think there is a way to do this that can actually significantly improve our ability to ensure the safety and security of that operating environment.

Senator SHAHEEN. Thank you. Thank you, Mr. Chairman.

Senator HOEVEN. Senator Baldwin.

INSPECTOR GENERAL'S RECOMMENDATIONS

Senator BALDWIN. Thank you. Let us start with the bigger picture. Mr. Roth, I remember when you testified before the Homeland Security Committee back in June, and I was struck with one of the things that you said in your testimony when describing how at the time TSA failed to concur with the majority of the inspector general's recommendations regarding vulnerabilities with the TSA's expansion of the PreCheck program. You said, "We believe this represents TSA's failure to understand the gravity of the situation."

Now, Mr. Neffenger, I know he was not speaking about you because you were not confirmed yet in this post at the time. And I understand that since that time you have agreed with a number of the inspector general's recommendations. But I am interested in your perspective on the gravity of the security situation that we face at TSA. And in light of the numerous security shortcomings identified by both the Government Accountability Office (GAO) and the inspector general, can you explain how you weight those and the necessity to address those shortcomings compared to other priorities that the TSA has identified internally in terms of you fulfilling your mission?

Mr. NEFFENGER. Well, the immediate priority is to address, I think, the findings of the inspector general. I absolutely agree with him that these were deeply disturbing and troubling, and I appreciate the fact that he did come forward right away, stopped the audit, and said we have got a problem here. And I know that the Secretary took that as seriously, as has already been mentioned.

So you have got to address that first because, first of all, I need to fix that. Second, I need to reinstate confidence in the traveling public that we know how to do our job. I think the good news is you can train out those kinds of failures. It is a matter of focus. I really do believe that we suffered from a shift in focus from the primary mission to one of efficiency. I understand where that came from. We were dealing with long wait times and a lot of dissatisfaction.

But if you are not careful, you can shift it in a way that leads to failure, and I think that some of what we saw was a result of that. So that is our immediate challenge right now. We have to fix that, and I have to test to make sure we actually got it fixed, and we are in the process of setting up that next series of tests to ensure that.

PASSENGER SCREENING: PERFORMANCE METRICS

Senator BALDWIN. I want to actually just stop you there because we come back over and over again to the pressure and the tension between your pressure to clear passengers quickly. I know the airlines are watching. Obviously passengers give you feedback on their experience and your vital security mission. One of the things we heard in our June hearing was just there are all sorts of metrics associated with the speed with which passengers are processed, and there are not as many except the absence of something really bad happening on the other side.

What more is being done to address that constant tension and pressure there? And I would ask both of you if you have comments.

Mr. NEFFENGER. So you have hit a real key point here, and I think it is one worth thinking about for a moment. You are right; there is a lot of tension. And the farther away you get from something actually happening in a system, the more people are inclined to just say, look, this is really just annoying, and I would like to get through this system quickly. I get that.

So I think there are some things you can do. First is you are right that there was this tension to collect metrics. You have got to pull the counting of people away from the people who are supposed to be making sure nothing bad gets through the system. So I do not want my frontline screeners counting people when what they really need to be doing is paying attention to what is coming through the system. Managers can do that, so you have distributed the duties where I think they belong.

There is a science to queue management, and I am learning more about that as I make my travels around. I actually talked to quite a few people about queue management, and I think we can learn some things. There are some best practices in the industry that I think we can do a better job of distributing. But I do not think queue management belongs in that frontline screener workforce. It belongs in a different location. So that is one thing that you can do.

Second is, I do think you can measure effectiveness even in the absence of something happening. I mean, that is in itself a measure, but it is not the only measure. You can look at the readiness of your equipment to operate, so it is all the equipment that we are fielding. Is it calibrated properly? Is it tested? Is it working at the same standards, and is it ready? So is there a readiness measure that you have? That is an idea I bring with me from my military service. You have an equipment readiness measure that says whether or not you are prepared to do the things you are being asked to do.

There is a system performance. Is the system performing? As you look at these measures across, do you see any gaps or any shortfalls? How is the workforce performance, not just the daily inject testing, but how are they being assessed because they go through regular assessment scores? Are you training them as they are supposed to perform, or are you using equipment that does not look like anything that they are going through? And that is some of the reason I want to get to some centralized training. And then, of course, what are you doing with respect to covert testing?

Then I think that there are some things—I have seen some innovative ideas for how you can improve efficiency while not taking your eye off of security. I mentioned I recently made a trip to visit with some counterparts in Europe. I was in the UK, France, and the Netherlands. And some of what they are doing in terms of creating multiple stations at the checkpoint to begin to divest, then placing yourself on the queue for the belt as opposed to following just a line of people allows you to move more people more efficiently through the system.

And as I have talked to some of the airports around the country that are in the process of looking to recapitalize their physical plant, I think we have an opportunity to try out some innovative designs there going forward. So I think it is a combination of measures that tell you whether or not you are ready to do your mission, and there are a number of those that I have enumerated that we can talk about.

And then it is how—when you do that—effectively can you move people through while yet resolving all those alarms. And there are some, I think, some simple changes that we can do over time to adjust the layout of the system that will move people more effectively through the system.

PASSENGER PROCESSING DURING SURGE TIMES

Senator BALDWIN. And, Mr. Chairman—I do not know if you are doing another round of questioning, because otherwise I do have one such suggestion to offer that I have gotten from feedback from my constituents.

Senator HOEVEN. We will have another round, but you can certainly go ahead depending on how long you think it will take.

Senator BALDWIN. Well, just let me comment on a situation that has come to my attention. Recently in my home airport, a lot of the equipment is allocated, the X-ray equipment in particular, based on passenger averages throughout a year. Certain communities have surge times when an exceptional number of people come through airports, whether it is a business that holds an enormous conference or I suppose in some areas it is sports team, et cetera. And the allocation of equipment does not take into consideration those surge times. And so, I would imagine that it would be able to help with both security and efficient processing—timely processing of passengers.

In our own case we have a conference that brings 10,000 people in through the airport in 1 week. It happens every year, and we know it is going to happen every year, hour and a half wait to get out.

Mr. NEFFENGER. That was the EPIC convention, right, recently? I have heard of it.

Senator BALDWIN. It is a double entendre in this case.

Mr. NEFFENGER. So I have asked our local FSD to meet with the airport director out there. I think that there—you have to be careful. You do not want to staff to the possible level that does not occur very often because then you have staff and equipment that is in excess of what you need. But I think that there is a middle ground there, and I like that idea of working with it.

And there may be a way to surge some things in for expected, particularly if there is something that happens on a regular routine basis. You know it is going to happen. It is no different than a reserve workforce that says we are going to have to do a lot of extra work around the Christmas holiday and around the Thanksgiving holiday, so you bring in a reserve staff.

So here is what I will tell you. Let me look at that. I know that I have asked our local Federal Security Director to talk about that, and I will follow up on some suggestions I think that will come out of that as well.

PASSENGER SCREENING: PERFORMANCE METRICS

Senator HOEVEN. Administrator, I want to go back to the testing, tracking, and metrics. So as you implement these changes to training people, to updating your procedures, and to technology, how are you testing and how are you measuring that result? Because this is something that I want to continue to follow up with you, not just at this hearing, but as we go forward so we know whether the changes that you are making in fact accomplish the objective. And I am going to ask Mr. Roth this same question.

Mr. NEFFENGER. Well, as I said, there is a readiness standard that we want to create in the equipment, and by that I mean I want to know if we have standards to which we expect equipment to operate, then I want to measure to those standards on a consistent basis. So one measure is, can I verify that every piece of equipment, AIT machines in particular, I have out there is actually performing to the standards I expect it to, and then what is the nature of that verification, so that there is a testing nature to that verification? So that is one measure of effectiveness for the equipment itself.

Then I want to understand how my workforce is performing with respect to moving people through it. So if I can verify that the equipment is performing to its highest capability, or at least to the capability we expect it to perform to, then I need to make sure that the person who is operating that piece of equipment operates it to its highest capability, and that they understand what they need to do when that equipment poses a challenge in the form of an alarm or something else. And they also have to understand when that equipment is not working.

So how do you do that? There are injects that you put into it. You can make the machine operate improperly and see if you have trained people to catch that. They should be trained to catch that. You can also do additional covert testing whether internally or through the inspector general to measure the performance. And there is an overall performance of the system as a whole. So as you do in the individual case, then I need to be able to see that in aggregate across the system whether that is within a given airport or multiple airports because I need to know what my variation and variability is across the system.

So what I have asked my staff to do is to develop a series of, for lack of a better term, what I call dashboard measures across the board for TSA effectiveness in the aviation environment in particular. And those measures would be a measure of readiness of equipment and readiness of people, and both are measures of

whether they have been trained. That is one measure. I check the first block. And then there are measures of whether they have been tested on their training, and then how have they performed on that testing, and then what is the variability in my workforce because that helps me determine whether or not my training is actually effective for what I do.

And then we measure what to do with respect to testing the system in a real-world environment. So assuming that I think my equipment is ready and the people are ready, because they seem to be performing well in a test environment, now what happens when I put them to the real test when they do not know if somebody is coming through? This is not a game, and they have got to catch somebody coming through.

There are lots of obvious details associated with that. I am not sure if that is responsive to your question, but that is kind of a large measure of the way in which I look at it. System readiness, system performance, workforce readiness, and then workforce performance are my overarching measures, and then the subcomponents of those to answer those questions.

Senator HOEVEN. So you said standards in each of those areas, and then you test to those standards.

Mr. NEFFENGER. Yes, sir. And the other thing is you test whether the standards are appropriate because I may set standards and then discover that my standards are inappropriate, and I may find that out because something just got through the checkpoint, or I may find that out because somebody has performed to standard, but they still have not found something. So in some cases on some of the tests, if you find that a process is not effective at finding a threat item, then my standard is no longer—is the wrong standard, and I have got to adjust that.

So you have to have a way to not just set the standards and assume you got them right, but to set the standards and then test your standards as well. So there is a component of this that assures that you are constantly testing the things that you say are the most critical to do.

Senator HOEVEN. Have you set those standards in each of the three areas—people, procedure, and technology—and have you set the overall standard?

Mr. NEFFENGER. We have set many of those standards. I am not where I want to be yet. We are still working on those. Part of that is as we look at what the Tiger Team results are, and I expect the actual full final report by the end of this month. I will be sharing that with this committee so that you will have it, and we would look forward to the opportunity to actually come up and walk you in detail through the findings.

Those findings are showing us exactly where we need to address our standards. I think we have some standards that are fine and that are appropriate, and I think we have some that need to be developed still as we look toward getting this. I want to get the immediate challenges corrected because I need to put confidence back in the system.

I am confident in the system. I am confident that a lot of the training that we have done already has dramatically improved our ability to catch threat injects coming through. We will test that

over the coming months. I am confident that the system is safe and the system is working. But I want to work hard on creating a deliberate process for continuously reviewing the standards and the training that we need to manage and to maintain those standards, the equipment that we need to meet the standards that we set, and then a review process that allows us to continually adjust those standards over time so that you do not just set it and forget it.

My great fear is that, particularly in an environment where security is of the greatest concern and in an environment that we have, when you have an evolving, and adapting, and learning enemy, you have to have an evolving, adapting, and learning system. And the day that you set a security system and say I got it right is the day you begin to lose the system's effectiveness.

Senator HOEVEN. Mr. Roth, would you respond to that both in terms of the standards and Administrator Neffenger's sense that the system is safe, although it needs to be continuously improved and adapted as the threat changes?

Mr. ROTH. Certainly. One of the things that we found during the audit process was that there were actually no metrics in place for the FSDs, the Federal security directors, at the airports involving safety. All the metrics regarded throughput and wait times and those kinds of things as opposed to safety. So, of course, you get what you measure, and what we got was the results of our covert testing.

We do a number of things to try to establish metrics, one of which obviously and the most visible one is the covert testing. We believe there is a value there because it is real-world testing. It takes the machine out of the lab and puts it into an environment that is likely to be the thing that will have to be measured. So we do our own covert testing.

The other thing that we are going to rely, I think, a little bit more heavily is on TSA's own internal covert testing that they do. We have already taken a look at it to determine whether or not it is reliable and trustworthy under sort of our own internal auditing standards, and we will be working with those teams to make sure that that system is something that is reliable because I do think that is the best sort of real-world measure of whether or not you are succeeding is these kinds of covert testing. Just like the best measure of a football team is how they do on Sunday, the best measure of the system as a whole is going to be whether or not they get through.

We are also going to be doing verification reviews. I alluded to the 115 different audits and inspections that we have done. Many of those are closed. For example, we did one on the behavior of detection officers, and one of the things that we found was that there were not any established metrics. And there were some issues with training and a number of other things. GAO did a similar report with regard to the science of behavior detection. Those recommendations are closed.

We are conducting a series of verification reviews that basically say we are going to look at that again and see whether or not those recommendations made sense at the time and whether it has fixed the problem that we have identified. So that is the other thing that

we are going to do, particularly in the area of metrics, for example, with the behavior of detection officers.

With regard to your question as to whether or not the threat is or the response to the threat is sufficiently—

Senator HOEVEN. Right, and let me stop you for just a minute. Your sense of the immediate threats or problems that you identified and how well those are being addressed? Are they being addressed? What is your sense of that, the immediate threats issues that you identified?

Mr. ROTH. Certainly the response has been everything that we could have hoped for. I do not think I could imagine a scenario where they are taking it more seriously than they are taking it now, and they are putting steps in place. Now, as an auditor I cannot say that those steps are effective because we have not done any continuation testing with regard to it. But if what we are measuring is output, that is, are they making changes, are they engaging in training, are they tightening up the rigor by which they are looking at checkpoint operations, I would have to say that it is as fulsome as I have seen or could hope for.

But as an auditor, tests matter, and we are going to be continuing to do tests on this, and then we are going to see exactly how effective they are.

Senator HOEVEN. Right. So it is really important that these standards are put in place and that you are testing to those standards right now. And, of course, we follow up on it through the inspector general. Senator.

EXPEDITED SCREENING

Senator SHAHEEN. Thank you. I want to go back to the security versus efficiency question because over the past couple of years, TSA has moved away from a one-size-fits-all approach, and I for one have thoroughly enjoyed being part of the PreCheck system. It has gotten me through airports much faster, and I appreciate that. I know the Global Entry Program is designed to do the same thing.

So, but I also understand that you are looking at some of the other efforts around expediting screening like managed inclusion, and are planning to dial those back. So can you talk a little bit about that decision? And then I want to make the connection of what this is going to mean for resources. And I think you alluded to this a little bit in your testimony because while I agree security is the number one priority, I have been in a lot of airports where people feel like efficiency is also important. And so, how do we balance those?

Mr. NEFFENGER. Thank you, Senator. And you are right, there is a balance needed because you also do not want a lot of people packing up outside the airport. That poses its own challenges. I think you can find that balance, I really do, but it starts with remembering what the primary mission is.

So I am a huge fan of a risk-based approach to security. We all know just intuitively that nearly everyone traveling through the system is safe to do so. And, because we know that, those who would harm the system are few in number if not focused intently on their desire to do damage. So I think—and I am a big fan of a vetted population. The more I can know about an individual who

arrives at a checkpoint, the safer we all are, and the more I do not have to worry about that individual as a risk to the system.

You alluded to the managed inclusion. Managed inclusion, as you know, is the practice of taking people who are not part of a pre-vetted population and randomly assigning them to an expedited screening line as a way of improving efficiency in a checkpoint operation. And there were some other randomized things that were done to them, exposure to trace detection and other things, and perhaps sometimes a pat-down that would assure you that they were safe to do so.

I think not just the covert testing results, but our own internal review of that tells me that that was introducing greater risk into the system than we were willing to accept. So that process is stopped. As of September 12, we no longer do that. That had represented about 14 percent of the daily traveling population—through that randomized assignment that were being put into expedited screening lines. So that has been turned off.

Where we still use a version of that is where we have bomb sniffing dogs, passenger screening canines. Some of you may have seen these at Dulles Airport. These are dogs that are trained to detect the traces of explosive vapors that may be emitted by someone who has been handling or otherwise been around explosives. Where we have those teams in place, we will continue to use a version of managed inclusion.

I am also working with the existing vendor, contractor who is doing the PreCheck enrollment to look for opportunities to expand that into retail environments outside the airport environment. We are, I hope, within days or weeks of putting out the request for proposal, which would allow up to three private-sector vendors to jump into the enrollment process. We are also looking at changing some of the enrollment—

Senator SHAHEEN. Can I just clarify what you are saying?

Mr. NEFFENGER. Yes.

Senator SHAHEEN. So up to three private sector vendors who would actually clear people on behalf of—

Mr. NEFFENGER. They would not clear on behalf of. They would do the initial enrollment. TSA always retains both the statutory responsibility and the requirement to do the actual vetting. But what they would do is collect the basic information necessary, submit it to the Federal Bureau of Investigation (FBI), and submit it to the TSA. And then FBI and TSA working together would run the names through the various clearance processes. But it would just provide more opportunities for people to participate.

I have also worked with the airlines and some of the travel groups, like the online travel companies, to do more marketing of the program. And I have been working with my other counterparts in the Department, Customs and Border Protection in particular, to look at a way to make things like global entry, PreCheck, Nexus, and Sentri more understandable and comprehensible, and more of a one-stop-shop, so that there is an understanding of what do I get when I pick one of these items.

I think that we can dramatically increase that population over the coming year to two years if we can move forward on some of these initiatives. I think that is the best way to start to really re-

duce risk in the traveling population. It also allows all of us to focus more intently on the people we do not know much about.

So if you think of a frequent traveler as somebody, and this will not sound like a frequent traveler, but who travels just three times per year on average if you are traveling in the air—that takes care of about 50 percent of the traveling population. So if you can get a large percentage of those people to sign up for PreCheck, then you could dramatically change the whole screening operation, screening environment.

Senator SHAHEEN. I have a number of other questions, but my time is up, so.

Senator HOEVEN. Senator Baldwin.

Senator BALDWIN. Thank you. I wanted to wade back into the discussion we were just having on behavior detection officers. In particular, I think it is known as the SPOT Program, the Screening Passengers by Observation Techniques Program. And if I understand correctly, the scope of the program is about 3,000 employees involved at a cost of about nearly \$900 million over a 5-year period between 2007 and 2012.

And I guess I just want to understand if what we are getting for that significant investment if concerns have been raised. Mr. Roth, I heard you speak about the audit and that audit is now closed. But could you remind us of some of the deficiencies that you found in the selection and training of these behavior detection officers? And I know the GAO also commented about whether or not it has been effective, but I would like to hear some of the concerns that you raised, and then response about the priority we should have on the program moving forward.

Mr. ROTH. Thank you for that question, and this is a concern that I had since I started this job. The audit was done before I arrived, and many of the recommendations had been closed out before I arrived. But functionally, the audit itself said that there were no performance measures, so we were not exactly sure what it is that we were getting for the investment. And you were right; my recollection is about 3,200 full-time equivalents (FTEs) at any given time who are doing this work.

And the idea is a good one, and I think it emulates what occurs in some, for example, European airports and some Middle East airports with regard to this idea that you want to have a population within TSA who can look somebody in the eye, similar to what our Customs officers do when they are admitting entry. And I think in my written testimony I talk about some successes that we have had in actually keeping terrorists out basically based on behavior detection.

But there are real questions as to whether or not this workforce, which is a massive workforce, is appropriately trained. Certainly our audit had seen that there was one group of training, and then basically there had been no refresher training. GAO, I noted, had some real concerns as to the level of sort of education, sophistication of some of the BDOs who were taking what are inherently flexible and subjective criteria and applying them against a vast population. It requires, I think, a bit of sophistication to be able to do that, and we were not comfortable with the fact that they had the population that would be able to do that.

So this is something that we are going to be looking at as we go forward. We are going to take a look at that audit and look at those recommendations, and see whether or not those recommendations actually fix the problem that we had seen. And if it is not, then we will make further recommendations.

BEHAVIORAL DETECTION PROGRAM

Senator BALDWIN. Mr. Neffenger, I am very interested to hear your reaction to your understanding of that audit and the value of that program vis-a-vis other priorities that you have.

Mr. NEFFENGER. Well, thank you, Senator. And this is a fair question and an appropriate question. Let me just start with a general comment before getting specific. In general, if this is a tool I can have in my security toolkit and it works, then I would like to have it because I like the idea. And I know that there are law enforcement agencies worldwide that look at behavior of individuals.

It is not a perfect answer, but these are indicators only. So whether you are a cop on the beat or you are working at a higher level of security professionalism, there are things that I think they will tell you that they rely upon to indicate whether or not they should just ask some more questions of somebody if nothing else. So in just a generalized statement, I think that it is worthwhile to consider it.

Now, have we implemented it correctly in the TSA? I will tell you that we have come down considerably in our numbers in that program. It has been reduced by about 15 percent in terms of actual bodies over the past 3 years. And the name has changed over time. It is still basically the same idea.

So when I was recently in the Netherlands, the Netherlands has their version of a behavioral detection program that they run their frontline officers through as well. And I told them that, first of all, I would like to understand how they do it. I would like to look at their training, and I would like to see whether we can benchmark against that. I have also talked to a number of large law enforcement agencies near our police department—L.A. Police Department. These are agencies I have worked with in the past, and said I know you do some version of this training for your people.

So I think I would agree with Inspector General Roth that there is more work to be done to determine the effectiveness of this, what are the measures you put in place to determine that effectiveness, can I base it in validated criteria that are validated by a third party. We have done some of that. I know that in response—again, this is prior to my arrival, but in response to some of the previous concerns and recommendations that we did do an—not TSA internal, but the Department's Science and Technology Branch did a validation of it, and there was a report recently provided to Congress.

But here is what I will say. I think that it is one of the areas I am going to look at hard in the coming months. As I said, my first priority was to get through this covert testing business, but then I want to look at all the aspects of TSA because I want to make sure that we are spending money that is provided by the taxpayers in the most effective way to ensure the security of the system.

I would like to think that behavior detection is an important element of that system. I think it can be. But I want to make sure it is benchmarked against worldwide standards. I think that they are out there. So I am looking forward to working with police departments that are doing this. I am looking forward to working with other like agencies, our counterparts in Europe that are doing this to see what they are encountering, how are they doing it, and can we benchmark against them, and have they done any studies of their own that might indicate where we are going. And then I want to take the training myself just to figure out what I think of it. And then I will get back.

So my jury is out. If I can come back to you with an assessment after I do all that.

STAFFING: PEAK FLIGHT TIMES

Senator HOEVEN. Administrator, the airports have peak flight times and off-peak flight times, so if you go through a checkpoint at a time when they have a whole lot of flights arriving and departing, or particularly departing, you can have very long lines. I mean, if you think in terms of a static workforce versus off-peak times, and that varies throughout the day. How are you handling that in terms of your workforce? You need a lot more people certain times during the day than you do other times. How are you handling that, because this goes to both safety and convenience issues?

Mr. NEFFENGER. Well, you implied one of the real challenges, and that is how to size yourself appropriately when you have such disparity in terms of throughput in any given day? Some of that is done with the part time workforce, so you use—and there is a good reason to have a certain number of people working part-time because you do have these big peak periods, and you bring the part-time workforce in to help you cover those peak periods, and then you move them off during your non-peak periods.

The other thing you can do during the non-peak times—then you are going to still need a certain baseline workforce just to manage it, and they are going to be available to you during those off-peak times. That is a good time to do some of the refresher training, some of the ongoing skills training, some of the focus on the mission piece that I think we need to do more of, and we need to do it more consistently across the organization. And then to focus our training on that piece.

So I think it is a continuing challenge, but one of the things that we are doing right now is looking at a true staffing model, not just an airport staffing model, but a true staffing model for the airport. Again, I think back to my experience in the Coast Guard, you start with, okay, if I have got a boat, how many people does it take to operate that boat? And then when it is a bare minimum necessary, first of all? You know, I need somebody to drive it. I need somebody to run the engine. I need somebody to throw off the lines. And then, once I have got that down, then what do I expect that crew to have to do, and how extreme might what I ask them to do be. So then how many additional people might I need to have on board or might I need to vary the size of that crew over time?

That is the same approach we are taking to TSA, and over the course of the past number of months, we have been looking—we

have been disassembling the entire staffing model to say did we get it right? What does it take to operate a checkpoint, and what are the true duties of those people at the checkpoint, and how are those duties distributed? Are there opportunities to combine some of those duties? We have found some opportunities to combine those for greater efficiency.

And then, what do you do about true peak travel times, whether it is holiday peak travel, which is its own set of challenges, or it is just peak travel throughout the day. As you know, you can watch DCA (Ronald Reagan National Airport). Between 6:00 and 8:00 in the morning, and then 4:00 and 8:00 in the afternoon is when all the activity seems to happen, and then it is just dead throughout the remainder of the day.

I can come back to you with examples of how we are doing that and would be happy to do so, and just show you how some of those staffing models work, and how you try to find the sweet spot so that you do not overshoot and wind up with too many people. But you also are sized such that you do not have extensive wait periods to get through during those peak travel times.

STAFFING: TRAINING

Senator HOEVEN. So that would indicate some need for part-time people, as you indicated. Your turnover rate is about 30 percent, or at least historically there has been about 30 percent turnover of those part-time staff. Are you sure then sending everybody through FLETC (Federal Law Enforcement Training Center) is the way to go in terms of training? Do you need some other way to train in order to both manage your staff and do it in a reasonably cost-effective way?

Mr. NEFFENGER. Well, there is an ongoing training need, as you alluded to. The 30-percent rate is what we are seeing as turnover just in the first 6 months. That is higher than I would like to see it. It is somewhat consistent with the kind of new hire turnover you see in other operating agencies, although higher than the military or others. So there is a weeding out process that always happens in an agency.

Over time, my overall turnover rate runs around between 10 and 12 percent for our workforce. For the part-time workforce, that number is around 20 to 25 percent over time. I understand the concern.

I do think that you can reduce turnover the more you connect and engage somebody with the mission of the organization. I do not think there is any substitute for consistent, baseline, foundational training to create a professional workforce. I think that over time as you do that, you will connect that workforce more directly to the mission, and they will feel more engaged.

So as you look at a world-class training facility like the Federal Law Enforcement Training Center down in Glynco where we have the opportunity to take existing structure, the intermodal facility that was built by FAA a number of years ago that has an airport operating environment in it. And you can put the actual equipment that they will be training on, and you can train real-world scenario-based training with play actors from the community.

FLETC has worked with the local community, so you can create a true airport environment, and you can do true scenario-based training. You can train everything from just day-to-day checkpoint operations to even active shooter training and the like. You can do it while not taking time away from the true real-world environment, and you can do that in a way that connects them to the culture of the organization, the mission of the organization, and an environment in which they are dealing with other professionals from around the country.

You can provide them with a certificate that certifies them as a professional, and you can do that in a consistent, repeatable, demonstrable, and measureable way. I do not think there is any substitute for that. When you then put them out into the field, now you have connected them to an organization that is larger than just the airport that they are all going to. We are already moving a lot of people around to about 75 different locations around the country to train, so the marginal cost is actually relatively small for, I think, what could be potentially a huge game payoff.

The business case that I am going to present to you actually spells this out in a more elegant way than I just did, but I think it can show that there is a way to measure what some people say is the intangible esprit de corps and connectedness that you get when you do that. And then that also frees up the airport environment to do that kinds of airport-specific skills and operational training that they need to be able to do that they are having a challenge doing right now.

But when I have compared the syllabi that is the currently in the on-the-job training environment to what we intend to do at the Federal Law Enforcement Training Center, from my perspective, there is no comparison; you know, going to true scenario-based as opposed to online training, actually seeing what happens when the kinds of explosives that we are concerned about detonate, the kind of damage they do as opposed to just watching a video. All I can say is the impact is significantly greater, and I believe that if we invest in our workforce in that way that we will get a greater investment back from that workforce in terms of their commitment to the organization.

Senator HOEVEN. Senator Shaheen.

STAFFING: MANAGED INCLUSION

Senator SHAHEEN. Thank you. I know we have got a limited amount of time left, but I wanted to go back to the managed inclusion. And as you referenced, that is going to require additional screeners because they are going to be more people now in the lines. And what do you anticipate for additional personnel that will be required?

Mr. NEFFENGER. Just as a reminder, we have come down about 5,600 screeners since 2011, and we were targeting a number in fiscal year 2016 that would have reduced us by about another—let us see. I am trying to think. I will not get the number right, but another 600 or 700 people. What I am asking to do is—and we have made significant progress toward that number that we planned in fiscal year 2016.

What I am asking to do is to halt right now at the summer 2015 levels, which would put us below our fiscal year 2015 actual numbers on board, slightly above by about 600 or so the numbers that we had planned to attain in fiscal year 2016. So this really is halting a further reduction, not necessarily adding new bodies, although it is more than we would have predicted in our fiscal year 2016 budget.

And so, I am asking to hold on to that while still taking reductions in other areas. We are still taking the BDO, the behavior detection officer, reductions. We are still taking savings with—that we get as a result of additional inline baggage systems that are being installed, so that allows us to save some FTE. And we are taking some savings as a result of fewer advanced imaging technology machines out there. So those continue.

But this is specifically with respect to the screening workforce. And what I need to do, the reason I am asking to hold is I need to evaluate whether or not we have got it right on the answer as we try to build the PreCheck population, the truly vetted population. I do not want to get to the point where I have excessive times because I have overshot while we are building up that population.

So this gives me—this buys me a year to work on the expansion of the vetted population to ensure that we get right the response to the covert testing failures. And then to work through the staffing models that we are doing to determine what the actual staffing has to be in the future. But the reminder is we have already come down significantly in the size of the workforce over the past 4½ years.

SCREENING TECHNOLOGY

Senator SHAHEEN. So you talked about the technology and we know about some of the shortcomings of the advanced imaging technology. What other technologies are you looking at in the future that can be helpful as we are screening passengers? Are biometrics something that you are thinking about?

And then, I understand that there are a limited number of fairly large companies that do the kind of technology that has been used today. Coming from a State where our foundation is all small businesses and they are doing a lot of innovative work, how can we encourage those small businesses to provide some of the innovation that TSA is going to need?

Mr. NEFFENGER. I will start with your last point first, Senator, because I think that is an important one. I would love to find a way to incentive small business to participate more often, and more completely, and more effectively in this system. As you know, there are large start-up costs to people who want to get into this, particularly in the research and development side. And we are somewhat hampered by the fact that many of these systems are propriety in nature, whether we are talking the software, the architecture, or the hardware itself. So I think there is a way to approach that.

I think there are things we can do that could incentivize small businesses. I think that there are more public/private partnerships that we can do when it comes to research and development and developmental testing. I have had some conversations already. With-

in the Department, I have talked to some of my former colleagues over at the Department of Defense, who have programs where they do this, you know, DARPA-like things where you can incentivize the private sector to come up with ideas.

Senator SHAHEEN. The SBIR Program is one of those that—

Mr. NEFFENGER. Exactly. I am hopeful that we can find some opportunities going forward. So I am trying to activate all the people who can think like this and can bring ideas forward. But I think we need to do something because it is never healthy to rely upon one or two major vendors as good as they might be. But going back to my comment that you cannot spend enough time thinking about this and evolving the system. I want to get some of the small innovative companies involved as well, particularly in the realm of software and other technology designs that could be useful.

That said, what are the kinds of technologies that I think we can look to in the future? I think we could—a more integrated experience going through, so in other words, you ought to be able to test shoes without taking them off their feet. I have seen some designs that allow us to do that.

Senator SHAHEEN. Yes, thank you. That would be very nice for all the women in high heels.

Mr. NEFFENGER. Yes, I know. If you talk about efficiency of the system, that extra few seconds it takes to both remove shoes and put them back on can be challenging. Same thing when you are removing belts, and jackets, and so forth. And I have seen prototype equipment out there that can address that.

I am encouraged by some of what I have seen with respect to increasing the resolution ability of the existing equipment as well as what it might look in the future. For biometrics, the Europeans are doing some interesting things with kind of real-time iris scanning that will connect them. Now, that raises issues for us here obviously if you start looking at—collecting biometrics on people. But I do think that there comes a time in the future where your fingerprint becomes your boarding pass, and it ties you directly to the ID that you present.

We have got technology that we hope to be rolling out that you have already funded. It is card authentication technology, which in its trials out at Dulles; it has shown real promise. And if you are familiar with this, this is the machine that reads an ID and determines whether or not it is actually a valid and not a counterfeited ID. It ties the individual who presents it, or at least it ties the ID to a validated boarding pass on the day that you are traveling, and it checks it against certain requirements.

I think the next step is to then validate that the ID is, in fact, attached to the person who presented it. But ultimately you can get away from the whole boarding pass piece entirely, and that will, I think, dramatically improve our understanding of who is presenting themselves at the checkpoint. It will tie them to a vetted population if you have one already. If you are already part of that population, it will connect you to the secure flight system and it is a real-time validation where you are going.

Then I have seen a lot of talk about—people have said things like screening at the speed of light for the security point of the future. All those are artful terms that are really just to indicate that

there is a security system out there that I think looks very different from the one we have, but that would require a huge investment to get to. I think the opportunity to try some of these things out is where you have airports, as I mentioned before, that are doing something new and innovative.

So I have talked to Denver about this, and I am interested in talking to LaGuardia as they think about recapitalizing, and some other airports—

Senator SHAHEEN. Please, that would be great.

Mr. NEFFENGER. [continuing]. To see an opportunity to do something different. And I think if you even do a couple of key demonstration projects, then it may create—first of all, it gives us a test bed, and it may create an opportunity for us to look for things like that in the future.

Senator SHAHEEN. Thank you.

AIR MARSHALS

Senator HOEVEN. I think you have covered most of the questions that I had. Maybe one I would finish up with is your plan for the Federal Air Marshals.

Mr. NEFFENGER. Well, let me start by saying I am really encouraged by the new director of the air marshals, Rod Allison, and his plan. What I have asked him to do and actually what he undertook even before I should say I asked him to do it—I am encouraging that he continue with his plan because he had this plan before I was confirmed—to really examine the entire air marshal operating concept. I think it is a good idea 14 years after the attacks of 9/11 to determine whether or not we are still positioning ourselves properly in all aspects of what we do.

I like having a badged law enforcement officer capability within TSA because I think there are unique challenges to the transportation system that can be addressed by having a law enforcement capability within the system. I know that Director Allison has looked really hard at the current employment deployment and strategy for the Air Marshals. He is working on developing a true staffing standard. We have never had a true staffing standard for the air marshals. I want to know what it takes to do what we need to do.

I will tell you that there are things that air marshals do currently on aircraft, which I can provide you in a classified setting that tell me that some capability like that is always going to be necessary. The question is beyond that, what else are we doing with them? And then how can we create other opportunities within the Air Marshal Program, whether it is the VIPR teams—visible intermodal protection and response teams—those interagency, law enforcement teams that look at other modes of transportation and other aspects of the transportation system.

So what I would say is, I think this is a good time for the air marshals because they have got a powerful, and visionary, and forward, and future-focused leader, who I think over the coming months is going to present me and oversight committees with a more compelling vision for them as well as at least a basis for discussion about the future of the Air Marshal Program going forward.

I will say this, we do need to get to a point where we can hire back into the program. We have been on a 4-year hiring freeze. A lot of the air marshals are aging out on mandatory retirement over the coming years. I think some 30 percent of that workforce will time out—for mandatory retirement age—within the next 5 years. And at a minimum I need to replenish that workforce with new people coming in. So I am hoping that we can get the hiring freeze lifted and begin to—at least hire into attrition rate in the program.

Senator HOEVEN. Senator Shaheen.

AVIATION SECURITY: GLOBAL

Senator SHAHEEN. I just have a final question, and that has to do with international travel because obviously as we look at the challenges we are facing from terrorist groups, thinking about how to address international travel and people coming into the country is a challenge. Can you talk about what you are doing in terms of working with other international airports and our countries around the world to address this issue?

Mr. NEFFENGER. That is a key point, Senator. I think I mentioned briefly in my opening statement that a consistent global approach to aviation security is critical because you do not want to create the opportunity to exploit differences and vulnerabilities that naturally exist if you have differences in your approach.

I did just recently return from meetings with my counterparts in the United Kingdom, France, and the Netherlands. This is a specific topic of conversation. We were also talking surface security in the wake of the recent attempted attack outside of Paris on the train into Paris.

But one of the things I wanted to do is first understand how security is over there. And if you have traveled internationally, you know that there are slight differences, some nuanced differences, and sometimes very dramatic differences in the way we do that.

There is an upcoming aviation security conference and international conference that I will be attending later in October, and a specific topic of concern for me is that we move toward a more globalized approach and a more globalized set of standards to aviation security.

There has been a lot of work done in that regard. I think there is a lot more that can be worked on, and I want to tie myself very closely to my international counterparts so that we do not introduce any vulnerabilities into the system that should not be introduced.

Senator SHAHEEN. Thank you. Mr. Chairman, I do not have any further questions, but I would just like to for the record acknowledge that we just had a very big visit in this country from the Pope. It was a huge national security issue, and we had a lot of law enforcement agencies involved in that, the Secret Service. And they did a really spectacular job, and I think it is important for us to acknowledge that.

Mr. NEFFENGER. And quite a few of our TSA screeners that were working on the frontlines.

Senator SHAHEEN. Thank you.

Senator HOEVEN. Thank you, Senator Shaheen. I would also like to acknowledge that Administrator Neffenger has made a real ef-

fort to reach out to airport administrators and the aviation industry. And I think that outreach effort has been well received. I think it is very important because, as you said, they are a very important part of the security and the safety of the screening as well as trying to do it in the most customer friendly manner for the traveling public. So I think that is certainly something that is to be commended.

I want to thank you, Administrator Neffenger. At the outset, Inspector General Roth talked about the need for a culture change in terms of addressing the problems that have been found. And what I hear him saying is that you have brought that mindset of making sure that any changes necessary to address the challenges and the problems are exactly what you are going to do, and work with your workforce to make sure that we are meeting the safety standards that we need to achieve, and doing it with the best convenience to the traveling public. And so, in that regard, the standards that you set, and your testing of those standards, are both vitally important.

And to the Inspector General, thank you for the work that you have done and the way that you have handled that work both immediately upon finding your results, but then also as follow up. And we will look for you for continued verification and follow up of the people, the technology, and the procedures that are being put in place, again, to achieve the safety that we want and the convenience that we want for the traveling public. So thanks to you both. Again, thanks to Ranking Member Senator Shaheen.

And with that, this subcommittee stands in recess. Thank you.

CONCLUSION OF HEARINGS

[Whereupon, at 12:54 p.m., Tuesday, September 29, the hearings were concluded, and the subcommittee was recessed, to reconvene subject to the call of the Chair.]