STATEMENT OF JOHN ROTH

INSPECTOR GENERAL

DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

CONCERNING

TSA: Security Gaps

November 3, 2015

Good morning Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee.

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

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

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

We may be in a very different place than we were in May, when I last testified before this Committee regarding TSA. 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.

Our Most Recent Covert Testing

In September 2015, we completed and distributed our report on our most recent round of covert testing. The results are classified at the Secret level, and the Department and this Committee have been provided a copy of our classified report. TSA justifiably classifies at the Secret level the validated test results; any analysis, trends, or comparison of the results of our testing; and specific vulnerabilities uncovered during testing. Additionally, TSA considers other information protected from disclosure as Sensitive Security Information.

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

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

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

- In September 2014, we conducted covert testing of the checked baggage screening system and identified significant vulnerabilities in this area caused by human and technology based failures. We also determined that TSA did not have a process in place to assess or identify the cause for equipment-based test failures or the capability to independently assess whether deployed explosive detection systems are operating at the correct detection standards. We found that, notwithstanding an intervening investment of over $550 million, TSA had not improved checked baggage screening since our 2009 report on the same issue. (*Vulnerabilities Exist in TSA's Checked Baggage Screening Operations*, OIG-14-142, Sept. 2014)

- In January 2012, we conducted covert testing of access controls to secure airport areas and identified significant access control vulnerabilities, meaning uncleared individuals could have unrestricted and unaccompanied access to the most vulnerable parts of the airport — the aircraft and checked baggage. (*Covert Testing of Access Controls to Secured Airport Areas*, OIG-12-26, Jan. 2012)

- In 2011, we conducted covert penetration testing on the previous generation of AIT machines in use at the time; the testing was far broader than the most recent testing, and likewise discovered significant vulnerabilities. (*Penetration Testing of Advanced Imaging Technology*, OIG-12-06, Nov. 2011)

The DHS Response

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

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

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

TSA has also been making significant progress on many additional, outstanding recommendations from prior reports.

The Importance of Independent Oversight

I have been gratified by the Department's response to our most recent covert testing 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. This review, like the dozens of reviews before it, was possible only because my office and my auditors had unfettered access to the information we needed.

As this Committee knows, our ability to gain access to information is under attack as a result of a recent memorandum by the Department of Justice's Office of Legal Counsel. This memorandum, purporting to interpret Congressional intent, comes to a conclusion that is absurd on its face: that the reference to "all records" in section 6(a) of the *Inspector General Act of 1978* somehow does not really mean "all records." The underpinning and backbone of our work – proven to be effective for more than 30 years – has now been called into question. The Department of Justice apparently believes that it is up to those being audited to determine what information gets disclosed. This is an inherent conflict of interest and upends the professional standards for auditors and investigators. Inspectors General need to follow the facts wherever they lead, and must have unfettered access to all of the agency's information to do so.

I believe I speak for the entire IG community in expressing my gratitude to this Committee for the legislation currently pending in the House, HR 2395, the *Inspector General Empowerment Act of 2015*. This legislation would fix the misguided attempt to restrict access to records, and would restore IG independence and empower IGs to conduct the kind of rigorous, independent and thorough oversight that taxpayers expect and deserve.

The legislation would also improve and streamline the way we do business. For example, it exempts us from some of the requirements when matching data from two or more data systems within the federal government. This will allow us to be able to complete some audits far more quickly than we would otherwise be able. For example, we conducted an audit that compared TSA's aviation worker data against information on individuals who were known to the Intelligence Community. Specifically, we asked the National Counterterrorism Center (NCTC) to perform a data match of over 900,000 airport workers with access to secure areas against the NCTC's Terrorist Identities Datamart Environment (TIDE). As a result of this match, we identified 73 individuals with terrorism-related category codes who also had active credentials.

According to TSA officials, current interagency policy prevents the agency from receiving all terrorism-related codes during vetting. TSA officials recognize that not receiving these codes represents a weakness in its program, and informed

us that TSA cannot guarantee that it can consistently identify all questionable individuals without receiving these categories. (*TSA Can Improve Aviation Worker Vetting (Redacted)*, OIG-15-98, June 2015).

Our audit broke new ground and was able to identify an area of significant vulnerability. However, under the current rules, it took *eighteen months* to receive authorization to match the data sets of the two agencies to look for overlaps. The *Inspector General Empowerment Act of 2015* would eliminate those barriers and equip us with an important and powerful analytic tool in our quest to identify waste, fraud, and abuse within the federal government.

TSA and the Asymmetric Threat

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

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

Mere Intelligence is Not Enough

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

In the vast majority of the instances, the identities of those who commit terrorist acts were simply unknown to or misjudged by the intelligence community. Terrorism, especially suicide terrorism, depends on a cadre of

newly-converted individuals who are often unknown to the intelligence community. Moreover, the threat of ISIS or Al Qaeda inspired actors — those who have no formal ties to the larger organizations but who simply take inspiration from them — increases the possibilities of a terrorist actor being unknown to the intelligence community.

Recent history bears this out:

- 17 of the 19 September 11th hijackers were unknown to the intelligence community. In fact, many were recruited specifically because they were unknown to the intelligence community.

- Richard Reid, the 2002 "shoe bomber," was briefly questioned by the French police, but allowed to board an airplane to Miami. He had the high explosive PETN in his shoes, and but for the intervention of passengers and flight crew, risked bringing down the aircraft.

- The Christmas Day 2009 bomber, who was equipped with a sophisticated non-metallic explosive device provided by Al Qaeda, was known to certain elements of the intelligence community but was not placed in the Terrorist Screening Database, on the Selectee List, or on the No Fly List. A bipartisan Senate report found there were systemic failures across the Intelligence Community, which contributed to the failure to identify the threat posed by this individual.

- The single most high profile domestic terrorist attack since 9/11, the Boston Marathon bombing, was masterminded and carried out by Tamerlan Tsarnaev, an individual who approximately two years earlier was judged by the FBI not to pose a terrorist threat, and who was not within any active U.S. Government databases.

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

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

Beyond the Checkpoint

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

Assessment of passenger risk

We applaud TSA's efforts to use risk-based passenger screening because it allows TSA to focus on high-risk or unknown passengers instead of known, vetted passengers who pose less risk to aviation security.

However, we have had deep concerns about some of TSA's previous decisions about this risk. For example, we recently assessed the Precheck initiative, which is used at about 125 airports to identify low-risk passengers for expedited airport checkpoint screening. Starting in 2012, TSA massively increased the use of Precheck. Some of the expansion, for example allowing Precheck to other Federal Government-vetted or known flying populations, such as those in the CBP Trusted Traveler Program, made sense. In addition, TSA continues to promote participation in Precheck by passengers who apply, pay a fee, and undergo individualized security threat assessment vetting.

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.

---

[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.

For example, I am pleased to report that TSA has stopped using one form of Managed Inclusion and has deactivated certain risk assessment rules that granted expedited screening through PreCheck lanes. However, TSA continues to use other risk assessment rules that we recommended it discontinue. We are communicating with TSA officials about these risk assessment rules; TSA recently told us it is reevaluating its position and we are awaiting formal documentation to that effect. I urge TSA to concur with our recommendations to address Precheck security vulnerabilities we identified during our review. As you may know, the House passed the *Securing Expedited Screening Act* (HR 2127), legislation that would eliminate Managed Inclusion altogether and limit risk assessment rules.

Access to secure areas

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

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

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

Other questionable investments in aviation security

TSA uses behavior detection officers to identify passenger behaviors that may indicate stress, fear, or deception. This program, Screening Passengers by Observation Techniques (SPOT), includes more than 2,800 employees and has cost taxpayers about $878 million from FYs 2007 through 2012.

We understand the desire to have such a program. Israel is foremost in their use of non-physical screening, although the differences in size, culture, and attitudes about civil liberties make such a program difficult to adopt in this

country. In the United States, sharp-eyed government officials were able to assess behavior to prevent entry to terrorists on two separate occasions:

- Ahmed Ressam's plot to blow up the Los Angeles International Airport on New Year's Eve 1999 was foiled when a U.S. Customs officer in Port Angeles, Washington, thought Ressam was acting "hinky" and directed a search of his car, finding numerous explosives and timers.

- In 2001, a U.S. immigration officer denied entry to the United States to Mohammed al Qahtani, based on Qahtani's evasive answers to his questions. Later investigation by the 9/11 Commission revealed that Qahtani was to be the 20th hijacker, assigned to the aircraft that ultimately crashed in Shanksville, Pennsylvania.

However, we have deep concerns that the current program is both expensive and ineffective. In 2013, we audited the SPOT program and found that TSA could not ensure that passengers were screened objectively, nor could it show that the program was cost effective or merited expansion. We noted deficiencies in selection and training of the behavior detection officers. Further, in a November 2013 report on the program, the Government Accountability Office (GAO) reported that TSA risked funding activities that had not been determined to be effective. Specifically, according to its analysis of more than 400 studies, GAO concluded that SPOT program behavioral indicators might not be effective in identifying people who might pose a risk to aviation security. TSA has taken steps to implement our recommendations and improve the program. However, we continue to have questions with regard to the program and this fiscal year will conduct a Verification Review, with regard to — among other things — performance management, training, and financial accountability, and selection, allocation, and performance of the Behavior Detection Officers.

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

TSA's role as regulator

TSA has dual aviation security 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. Concern exists about which entity is accountable for protecting areas other than checkpoints in relation to airport

worker vetting, perimeter security, and cargo transport. We have also assessed whether TSA is appropriately regulating airports, such as whether it ensures airports' compliance with security regulations. We have found shortfalls.

In the case of airport worker vetting, for example, TSA relies on airports to submit complete and accurate aviation worker application data for vetting. In a recent audit, we found TSA does not ensure that airports have a robust verification process for criminal history and authorization to work in the United States, or sufficiently track the results of their reviews. TSA also did not have an adequate monitoring process in place to ensure that airport operators properly adjudicated credential applicants' criminal histories. TSA officials informed us that airport officials rarely or almost never documented the results of their criminal history reviews electronically. Without sufficient documentation, TSA cannot systematically determine whether individuals with access to secured areas of the airports are free of disqualifying criminal events.

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

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

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

Conclusion

Making critical changes to TSA's culture, technology, and processes is not an easy undertaking. However, a commitment to and persistent movement

towards effecting such changes — including continued progress towards complying with our recommendations — is paramount to ensuring transportation security. We recognize and are encouraged by TSA's steps towards compliance with our recent recommendations. Without a sustained commitment to addressing known vulnerabilities, the agency risks compromising the safety of the Nation's transportation systems.

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

Appendix A
Recent OIG Reports on the Transportation Security Administration

Covert Testing of the TSA's Passenger Screening Technologies and Processes at Airport Security Checkpoints (Unclassified Summary), OIG-15-150, September 2015

Use of Risk Assessment within Secure Flight (Redacted), OIG-14-153, June 2015

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

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

Allegation of Granting Expedited Screening through TSA PreCheck Improperly (Redacted), OIG-15-45, March 2015

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

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

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

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

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-12-06	Transportation Security Administration Penetration Testing of Advanced Imaging Technology	11/21/2011	Recommendation includes Sensitive Security Information.	**Closed***	Agreed
OIG-12-06	Transportation Security Administration Penetration Testing of Advanced Imaging Technology	11/21/2011	Recommendation includes Sensitive Security Information.	**Closed***	Agreed
OIG-12-06	Transportation Security Administration Penetration Testing of Advanced Imaging Technology	11/21/2011	Recommendation includes Sensitive Security Information.	Closed	Agreed
OIG-12-06	Transportation Security Administration Penetration Testing of Advanced Imaging Technology	11/21/2011	Recommendation includes Sensitive Security Information.	Closed	Agreed
OIG-12-06	Transportation Security Administration Penetration Testing of Advanced Imaging Technology	11/21/2011	Recommendation includes Sensitive Security Information.	Closed	Agreed

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-12-06	Transportation Security Administration Penetration Testing of Advanced Imaging Technology	11/21/2011	Recommendation includes Sensitive Security Information.	Closed	Agreed
OIG-13-91	Transportation Security Administration's Screening of Passengers by Observation Techniques	5/29/2013	We recommend that the Assistant Administrator, Office of Security Capabilities develop and implement a comprehensive strategic plan for the Screening of Passengers by Observation Techniques (SPOT) program that includes— Mission, goals, objectives, and a system to measure performance; A training strategy that addresses the goals and objectives of the SPOT program; A plan to identify external partners integral to program success, such as law enforcement agencies, and take steps to ensure that effective relationships are established; and A financial plan that includes identification of priorities, goals, objectives, and measures; needs analysis; budget formulation and execution; and expenditure tracking.	Closed	Agreed
OIG-13-91	Transportation Security Administration's Screening of Passengers by Observation Techniques	5/29/2013	We recommend that the Assistant Administrator, Office of Security Capabilities develop and implement controls to ensure completeness, accuracy, authorization, and validity of referral data entered into the Performance Measurement Information System.	Closed	Agreed

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-13-91	Transportation Security Administration's Screening of Passengers by Observation Techniques	5/29/2013	We recommend that the Assistant Administrator, Office of Security Capabilities develop and implement a plan that provides recurrent training to Behavior Detection Officer (BDO) instructors and BDOs.	Closed	Agreed
OIG-13-91	Transportation Security Administration's Screening of Passengers by Observation Techniques	5/29/2013	We recommend that the Assistant Administrator, Office of Security Capabilities develop and implement a plan to assess BDO instructor performance in required core competencies on a regular basis.	Closed	Agreed
OIG-13-91	Transportation Security Administration's Screening of Passengers by Observation Techniques	5/29/2013	We recommend that the Assistant Administrator, Office of Security Capabilities monitor and track the use of BDOs for non-SPOT related duties to ensure BDOs are used in a cost-effective manner and in accordance with the mission of the SPOT program.	Closed	Agreed
OIG-13-91	Transportation Security Administration's Screening of Passengers by Observation Techniques	5/29/2013	We recommend that the Assistant Administrator, Office of Security Capabilities develop and implement a process for identifying and addressing issues that may directly affect the success of the SPOT program such as the selection, allocation, and performance of BDOs.	Closed	Agreed

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-13-99	Transportation Security Administration's Screening Partnership Program	6/20/2013	We recommend that the Transportation Security Administration Deputy Administrator expedite developing and implementing procedures to ensure that decisions on Screening Partnership Program applications and procurements are fully documented according to applicable Department and Federal guidance.	Closed	Agreed
OIG-13-99	Transportation Security Administration's Screening Partnership Program	6/20/2013	We recommend that the Transportation Security Administration Deputy Administrator establish and implement quality assurance procedures to ensure that the most relevant and accurate information is used when determining eligibility and approving airports' participation in the Screening Partnership Program.	Closed	Agreed
OIG-13-120	Transportation Security Administration's Deployment and Use of Advanced Imaging Technology	9/16/2013	We recommend that the Deputy Administrator, Transportation Security Administration: Develop and approve a single, comprehensive deployment strategy that addresses short- and long term goals for screening equipment.	Closed	Agreed
OIG-13-120	Transportation Security Administration's Deployment and Use of Advanced Imaging Technology	9/16/2013	We recommend that the Deputy Administrator, Transportation Security Administration: Develop and implement a disciplined system of internal controls from data entry to reporting to ensure PMIS data integrity.	**Closed***	Agreed

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-14-142	(U) Vulnerabilities Exist in TSA's Checked Baggage Screening Operations	9/9/2014	This recommendation is classified.	Closed	Agreed
OIG-14-142	(U) Vulnerabilities Exist in TSA's Checked Baggage Screening Operations	9/9/2014	This recommendation is classified.	Open - Resolved	Agreed
OIG-14-142	(U) Vulnerabilities Exist in TSA's Checked Baggage Screening Operations	9/9/2014	This recommendation is classified.	**Closed***	Agreed
OIG-14-142	(U) Vulnerabilities Exist in TSA's Checked Baggage Screening Operations	12/16/2014	This recommendation is classified.	Open – Resolved	Agreed
OIG-14-142	(U) Vulnerabilities Exist in TSA's Checked Baggage Screening Operations	12/16/2014	This recommendation is classified.	Open – Unresolved	Agreed
OIG-14-153	Use of Risk Assessment within Secure Flight	9/9/2014	Recommendation includes Sensitive Security Information.	Open – Resolved	**Agreed****

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-14-153	Use of Risk Assessment within Secure Flight	9/9/2014	Recommendation includes Sensitive Security Information.	Closed	Agreed
OIG-14-153	Use of Risk Assessment within Secure Flight	9/9/2014	Recommendation includes Sensitive Security Information.	**Closed***	**Agreed****
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Unresolved	Disagreed
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Resolved	Agreed
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Resolved	Agreed
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Resolved	Agreed
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Resolved	**Agreed****
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Resolved	Agreed

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	**Open – Resolved***	Agreed
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	**Closed***	**Agreed****
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Resolved	**Agreed****
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	We recommend that the TSA Assistant Administrator for the Office of Intelligence and Analysis: Employ exclusion factors to refer TSA PreCheck ® passengers to standard security lane screening at random intervals.	**Open – Resolved***	**Agreed****
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	**Closed***	Agreed
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	**Closed***	Agreed

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	We recommend that the TSA Assistant Administrator for the Office of Security Operations: Develop and implement a strategy to address the TSA PreCheck ® lane covert testing results.	Open – Resolved	**Agreed****
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Resolved	**Agreed****
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	We recommend that the TSA Assistant Administrator for the Office of Intelligence and Analysis: Provide an explanation of TSA PreCheck ® rules and responsibilities to all enrollment center applicants and include this information in eligibility letters.	Open – Resolved	Agreed
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	We recommend that the TSA Assistant Administrator for the Office of Intelligence and Analysis: Coordinate with Federal Government and private partners to ensure all TSA PreCheck ® eligible populations receive the rules and responsibilities when notifying participants of eligibility.	Open – Resolved	**Agreed****
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	We recommend that the TSA Chief Risk Officer: Develop consolidated guidance outlining processes and procedures for all offices involved in the TSA PreCheck ® initiative.	Open – Resolved	Agreed

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-15-45	Allegations of Granting Expedited Screening through TSA PreCheck Improperly (OSC File No. DI-14-3679)	3/16/2015	Recommendation includes Sensitive Security Information.	Open – Unresolved	Disagreed
OIG-15-45	Allegations of Granting Expedited Screening through TSA PreCheck Improperly (OSC File No. DI-14-3679)	3/16/2015	We recommend that the TSA Assistant Administrator for Security Operations: Modify standard operating procedures to clarify Transportation Security Officer (TSO) and supervisory TSO authority to refer passengers with TSA PreCheck boarding passes to standard screening lanes when they believe that the passenger should not be eligible for TSA PreCheck screening.	**Closed***	Agreed
OIG-15-86	The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program	5/6/2015	We recommend that TSA's Office of Security Capabilities and Office of Security Operations develop and implement a preventive maintenance validation process to verify that required routine maintenance activities are completed according to contractual requirements and manufacturers' specifications. These procedures should also include instruction for appropriate TSA airport personnel on documenting the performance of Level 1 preventive maintenance actions.	**Open – Resolved***	Agreed

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-15-86	The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program	5/6/2015	We recommend that TSA's Office of Security Capabilities and Office of Security Operations: Develop and implement policies and procedures to ensure that local TSA airport personnel verify and document contractors' completion of corrective maintenance actions. These procedures should also include quality assurance steps that would ensure the integrity of the information collected.	**Open – Resolved***	Agreed
OIG-15-86	The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program	5/6/2015	We recommend TSA's Office of Acquisition enhance future screening equipment maintenance contracts by including penalties for noncompliance when it is determined that either preventive or corrective maintenance has not been completed according to contractual requirements and manufacturers' specifications.	**Open – Resolved***	Agreed
OIG-15-98	TSA Can Improve Aviation Worker Vetting	6/4/2015	We recommend that TSA follow up on its request to determine if its credential vetting program warrants the receipt of additional categories of terrorism related records.	**Open – Resolved***	Agreed
OIG-15-98	TSA Can Improve Aviation Worker Vetting	6/4/2015	We recommend that TSA issue guidance requiring annual security inspection process to include verification of original documentation supporting airport adjudication of an applicant's criminal history and work authorization.	**Open – Resolved***	Agreed

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

OIG-15-98	TSA Can Improve Aviation Worker Vetting	6/4/2015	We recommend TSA pilot FBI's Rap Back program and take steps to institute recurrent vetting of criminal histories at all commercial airports.	**Open – Resolved***	No Response
OIG-15-98	TSA Can Improve Aviation Worker Vetting	6/4/2015	We recommend TSA require airports to put an end date to credentials of individuals allowed to work in the United States temporarily.	**Open – Resolved***	Agreed
OIG-15-98	TSA Can Improve Aviation Worker Vetting	6/4/2015	We recommend TSA analyze denials of credentials due to lawful status issues to identify airports with specific weaknesses, and address these weaknesses with airport badging officials as necessary.	**Open – Resolved***	No Response
OIG-15-98	TSA Can Improve Aviation Worker Vetting	6/4/2015	We recommend that TSA implement all necessary data quality checks necessary to ensure that all credential application data elements required by TSA Security Directive 1542-04-08G are complete and accurate.	**Open – Resolved***	No Response
OIG-15-150	(U) Covert Testing of the Transportation Security Administration's Passenger Screening Technologies and Processes at Airport Security Checkpoints	9/22/2015	This recommendation is classified.	Open-Unresolved	Agreed

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

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

Appendix C
Current and Planned OIG Work on TSA

Projects In-Progress:

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

Upcoming Projects:

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