STATEMENT OF JOHN ROTH

INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

CONCERNING

TRANSPORTATION SECURITY: ARE OUR AIRPORTS SAFE?

MAY 13, 2015

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, thank you for inviting me here today to discuss airport security issues.

TSA's mission—to protect the Nation's transportation systems to ensure freedom of movement for people and commerce—is incredibly difficult. First, it is a massive operation, with a budget of more than $7.2 billion in fiscal year (FY) 2015. Each day, TSA screens about 1.8 million passengers and about 3 million carry-on bags at 450 airports nationwide. Second, we face a classic asymmetric threat in attempting to secure our transportation security: TSA cannot afford to miss a single, genuine threat without potentially catastrophic consequences, yet a terrorist only needs to get it right once. TSA's 50,000 transportation security officers (TSO) spend long hours performing tedious tasks that require constant vigilance. Complacency can be a huge detriment to TSA's ability to carry out its mission. Ensuring consistency across DHS' largest workforce would challenge even the best organization.

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

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

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

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

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

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

Passenger and Baggage Screening

Risk Assessment Rules

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

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

- Granted PreCheck eligibility to other Federal Government-vetted or known flying populations, such as those in the CBP Trusted Traveler Program.

- Established and increased the PreCheck application program, which requires individualized security threat assessment vetting.

- Implemented risk assessment rules.

- Used "managed inclusion" for the general public, allowing random passengers access to PreCheck lanes without having assessed their risk.

As a result of our inspection, we concluded that the first two methods are sound approaches to increasing the PreCheck population, but the latter two create security vulnerabilities. Based on our review, we believe TSA needs to modify the initiative's vetting and screening processes. We also determined that PreCheck communication and coordination need

improvement. TSA did not concur with the majority of our 17 recommendations; we believe this represents TSA's failure to understand the gravity of the situation. (*Security Enhancements Needed to the TSA PreCheck Initiative, (Unclassified Summary) OIG-15-29*)

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

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

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

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

Passenger and Baggage Screening

Detection of dangerous items on people and in baggage requires reliable equipment with effective technology, as well as well-trained and alert TSOs who understand and consistently follow established procedures and exercise good judgment. We believe there are vulnerabilities in TSA's screening operations, caused by a combination of technology failures and human error. Since 2004, we have conducted eight covert penetration

testing audits on passenger and baggage screening operations. Because these audits involved covert testing and contain classified or Sensitive Security Information, we can only discuss the results in general terms at this hearing. However, we would be happy to schedule a private briefing with this Committee or staff to discuss the information we are not able to disclose today.

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

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

We are currently conducting covert testing to evaluate the effectiveness of TSA's Automated Target Recognition software[2] and checkpoint screener performance in identifying and resolving potential security threats at airport checkpoints. Once that testing is completed and evaluated, we will report our results to the Secretary and Congress.

TSA uses layers of security to prevent dangerous items or individuals from entering aircraft. In one layer, TSA uses behavior detection officers to identify passenger behaviors that may indicate stress, fear, or deception. This program, Screening Passengers by Observation

---

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

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

Techniques (SPOT), includes more than 2,800 employees and has cost taxpayers about $878 million from FYs 2007 through 2012.

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

Access Controls to Secure Areas and Workforce Integrity

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

Airport Badges and Access to Secure Areas

In February 2013, we identified problems with TSA's Aviation Channeling Services Provider project, which uses vendors to relay airport badge applicants' biographical information and fingerprints to TSA for vetting. Because TSA did not properly plan, manage, or implement the project, airports nationwide experienced a backlog of background checks. To address the backlog, TSA temporarily allowed airports to issue badges without the required background checks. Consequently, at least five airports granted badges to individuals with criminal records, giving them access to secure airport areas. In response to our findings, TSA agreed to develop a lessons learned report, establish a policy requiring all projects to include a comprehensive plan, communicate customer service expectations to vendors and monitor their performance for accountability, and require inspectors to review badges issued without the required background checks. (*Transportation Security Administration's Aviation Channeling Services Provider Project, OIG-13-42*)

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

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

Additionally, this month we will publish the final report from an audit we conducted of TSA's controls over the vetting of aviation workers possessing or applying for credentials that allow unescorted access to secure areas of commercial airports. Specifically, we assessed TSA's process for vetting workers for terrorist links, criminal history, and lawful status. We also sought to determine the accuracy and reliability of the data TSA uses for vetting.

Workforce Integrity

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

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

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

States. The TSO was sentenced to 87 months of imprisonment and 2 years supervised release.

TSA Operations and Management Oversight

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

Acquiring and Maintaining Equipment

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

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

Another recent audit revealed that the safety of airline passengers and aircraft could be compromised by TSA's inadequate oversight of its equipment maintenance contracts. TSA has four maintenance contracts valued at about $1.2 billion, which cover both preventive and corrective maintenance for airport screening equipment. Because TSA does not adequately oversee equipment maintenance, it cannot be assured that routine preventive maintenance is performed on thousands of screening units or that this equipment is repaired as needed, ready for operational use, and operating at its full capacity. In response to our recommendations, TSA agreed to develop, implement, and enforce policies and procedures to ensure its screening equipment is maintained

as required and is fully operational while in service. (*The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program*, OIG-15-86)

Use of Criminal Investigators

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

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

Cybersecurity

We have conducted a number of audits that highlight our concerns about TSA's management of its information technology (IT). During onsite inspections of IT systems, we found significant, repeated deficiencies in IT systems that support TSA's operations. These include insufficient physical security and access controls for numerous TSA server rooms and communication closets, failure to implement known software patches to servers, and other deviations from DHS IT policies and procedures. Collectively, these deficiencies place the confidentiality, integrity, and availability of TSA's data at risk. We are especially concerned that repeated deficiencies mean lessons learned at one airport

are not being shared with other airports. (*Audit of Security Controls for DHS Information Systems at John F. Kennedy International Airport (Redacted) (Revised), OIG-15-18*; *Audit of Security Controls for DHS Information Technology Systems at Dallas/Fort Worth International Airport, OIG-14-132*; *Technical Security Evaluation of DHS Activities at Hartsfield Jackson Atlanta International Airport, OIG-13-104*)

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

Conclusion

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

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

Appendix

OIG Reports Referenced in This Testimony

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

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

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

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

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

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

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

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

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

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

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

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

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