OFFICE OF INSPECTOR GENERAL

# Testimony of Inspector General John Roth

## Before the Committee on Homeland Security and Governmental Affairs

## United States Senate

## "Frustrated Travelers: Rethinking TSA Operations to Improve Passenger Screening and Address Threats to Aviation"

Homeland Security

**June 7, 2016**
**10:00 AM**

# DHS OIG HIGHLIGHTS

## *Frustrated Travelers: Rethinking TSA Operations to Improve Passenger Screening and Address Threats to Aviation*

**June 7, 2016**

## Why We Did This

The audits and inspections discussed in this testimony are part of our ongoing efforts to ensure the efficiency and effectiveness of TSA's operations.

## What We Recommend

We made numerous recommendations to TSA in our audit and inspection reports. Our recommendations are aimed at helping TSA improve its ability to execute its important mission.

**For Further Information:**
Contact our Office of Legislative Affairs at (202) 254-4100, or email us at DHS-OIG.OfficeLegislativeAffairs@oig.dhs.gov

## What We Found

This testimony highlights a number of our recent reviews:

- Since 2004, we have conducted eight covert penetration testing audits on passenger and baggage screening operations. Last summer, the results of our covert testing of TSA's Automated Target Recognition Software and checkpoint screener performance was troubling and disappointing.

- Recent audits reflect issues with TSA's stewardship of taxpayer dollars, including inadequate oversight of its equipment maintenance contracts; failure to develop a comprehensive deployment strategy for AIT machines; issues with TSA's administration of its contracts; and Office of Inspection's failure to use its staff and resources efficiently.

- In June of 2015, we found TSA lacked assurance that it properly vetted aviation workers possessing or applying for credentials that allow unescorted access to secure areas.

## DHS Response

TSA concurred with most recommendations made in these audits and inspections.

Chairman Johnson, Ranking Member Carper, and members of the Committee, thank you for inviting me to testify on TSA and threats to aviation.

Almost a year ago, I testified before this Committee at a hearing on TSA's programs and operations. During that hearing, I testified that "we remain deeply concerned about its ability to execute its important mission." I noted that TSA had challenges 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. At the time, I testified that TSA's reaction to the vulnerabilities that our audits uncovered reflected "TSA's failure to understand the gravity of the situation."

Since that time, we have conducted more audits and released more reports that challenge TSA's management of its programs and operations.

However, I believe we are in a different place than we were last June. As a result of our audit reports, and a vigorous response by DHS, TSA is now, for the first time in memory, critically assessing its deficiencies in an honest and objective light. TSA's leadership has embraced the OIG's oversight role and appears to be addressing vulnerabilities.

However, we should not minimize the significance of the challenges TSA faces, and the risk that failure brings. The task is difficult and will take time. In the meantime, my office will continue to conduct audits, inspections and investigations, and bring a professional skepticism to our review, as we are required to do.

**The Nature of the Threat**

The stakes are enormous. 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 about 2 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 simply encouraging lone wolf attacks – and posing a different type of threat. 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 ideally be carried out in areas where people are concentrated and vulnerable, such as the Nation's commercial aviation system.

**Checkpoint Performance**

Detection of dangerous items on people and in baggage requires reliable equipment with effective technology, as well as well-trained and alert Transportation Security Officers (TSO) who understand and consistently follow established procedures and exercise good judgment.

We have identified 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.

The most recent of these tests, conducted last summer, was designed to evaluate the effectiveness of TSA's Automated Target Recognition software[1] and checkpoint screener performance in identifying and resolving potential security threats at airport checkpoints. The specific results of our covert testing, like the testing we have done in the past, are classified at the Secret level. However, we were able to describe the results as troubling and disappointing. *(Covert Testing of TSA's Passenger Screening Technologies and Processes at Airport Security Checkpoints* (Unclassified Summary), OIG-15-150)

In contrast to previous covert testing reports, however, TSA's response to our most recent testing has been significant. DHS and TSA instituted a series of changes well before our audit was final. As part of that effort, TSA initiated a "tiger team" program to conduct a focused analysis on issues that the OIG had uncovered, as well as other matters. The result was a list of 22 major corrective actions that TSA has taken or planned to take. While 21 of 22 of the recommendations remain open, we are satisfied with the response we have

[1] 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.

seen at TSA. These efforts have resulted in significant changes to TSA leadership, operations, training, and policy.

We will be monitoring TSA's efforts to increase the effectiveness of checkpoint operations and will continue to conduct covert testing. In fact, we have a round of covert testing scheduled for this summer, and are presently developing the testing protocols. Consistent with our obligations under the *Inspector General Act*, we will report our results to this Committee as well as other committees of jurisdiction.

**Risk Assessment**

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.

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 it was assuming. I am pleased to report, however, that we have recently made significant progress in getting concurrence and compliance with these recommendations.

For example, I am pleased to report that TSA 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 broad risk assessment rules that we recommended it discontinue. We believe that expedited screening that is based on anything but an individualized assessment of the passenger presents an unacceptable risk to transportation safety. We have been communicating with TSA officials about this, and TSA has provided us a plan by which they will decrease reliance on this process. However, we remain concerned about the pace of progress in this area and will continue to monitor the situation.

**The Limits of Risk Assessment and its Implications on Budget and Passenger Wait Times**

In the past, officials from TSA, in testimony to Congress, in speeches to think tanks, and elsewhere, have described TSA as a risk-based, 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. Reliance on intelligence is a necessary thing, but we believe that TSA in the past has overstated the effect of reliance on intelligence and a risk-based approach.

The hard truth is that 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 with no previous experience in this area. 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. The majority US terrorist attacks were committed by individuals largely unknown to the intelligence community.

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.

Unfortunately, TSA made incorrect budget assumptions in 2014 and 2015 about the impact that risk-based security would have on its operations. For the Administration's FY 2016 budget, for example, TSA believed that it could reduce the screener workforce by 1,666 full time employees:

> RBS [risk-based security] methods have proven more efficient in moving people through the checkpoint than regular screening lanes and require fewer resources than a traditional screening

lane. This reduction reflects TSA's goal to continue transitioning to a smaller, more skilled, professional workforce capable of meeting the evolving requirements of RBS operations while ensuring the efficient movement of the travelling public.[2]

Likewise, in the Administration's FY 2015 request, TSA asked for a reduction of 1,441 full time screeners based on claimed efficiencies in risk-based security.[3]

However, our testing and audits found that TSA had been incurring unacceptable risks to transportation safety in its approach, and TSA eliminated some of the more dangerous practices that we identified. Moreover, we believe that even if TSA had not changed its approach to screening, the planned decline in the screener workforce was far too optimistic. As a result, the long lines we are seeing this summer are not mysterious: TSA, because of the decisions it made in 2014 and 2015, has fewer screeners but is facing more passenger volume than ever before.

**TSA Operations and Management Oversight**

Our audits reflect 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 equipment, including Explosives Detection System machines, Explosives Trace Detection machines, Advanced Imaging Technology (AIT) machines, information technology, Bottled Liquid Scanners, x-ray machines, and walkthrough metal detectors, yet a series of our audits found issues with TSA's acquisition management.

- Last month, we issued a report on TSA's Security Technology Integrated Program (STIP), a data management system that connects airport transportation security equipment, such as Explosive Trace Detectors, Explosive Detection Systems, Advanced Technology X-ray, AIT, and Credential Authentication Technology. This program enables the remote management of this equipment by connecting it to a centralized server

[2] DHS Budget in Brief, FY 2016, page 62.
https://www.dhs.gov/sites/default/files/publications/FY_2016_DHS_Budget_in_Brief.pdf

[3] DHS Budget in Brief, FY 2015, page 73.
https://www.dhs.gov/sites/default/files/publications/FY15BIB.pdf

that supports data management, aids threat response, and facilitates equipment maintenance, including automated deployment of software and configuration changes.

However, we found that, while progress has been made, numerous deficiencies continue in STIP information technology security controls, including unpatched software and inadequate contractor oversight. This occurred because TSA typically has not managed STIP equipment in compliance with DHS guidelines regarding sensitive IT systems. Failure to comply with these guidelines increases the risk that baggage screening equipment will not operate as intended, resulting in potential loss of confidentiality, integrity, and availability of TSA's automated explosive, passenger, and baggage screening programs.

TSA also has not effectively managed STIP servers as IT investments. Based on senior-level TSA guidance, TSA officials did not designate these assets as IT equipment. As such, TSA did not ensure that IT security requirements were included in STIP procurement contracts. This promoted the use of unsupported operating systems that created security concerns and forced TSA to disconnect STIP servers from the network. TSA also did not report all STIP IT costs in its annual budgets, hindering the agency from effectively managing and evaluating the benefits and costs of STIP. (*IT Management Challenges Continue in TSA's Security Technology Integrated Program*, OIG-16-87)

- 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)

- In 2013, 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)

- Also in 2013, we conducted an audit to determine TSA's progress in establishing key information technology management capabilities to support mission needs. We found that not all information technology procurements had gone through the information technology acquisition review process because they were not categorized as information technology procurements. As a result, there was little assurance that all information technology investments were aligned with the Chief Information Officer's strategy or TSA's future information technology mission needs.

  Additionally, we found that TSA's information technology systems did not provide the full functionality needed to support its mission due to challenges with TSA's requirements gathering process. The staff created manual workarounds or developed local systems to accomplish their mission. In addition, information technology support roles were not well defined or communicated, and the number of information technology support staff was not sufficient at certain field sites. Some field sites detailed employees from operational areas to fill in gaps in information technology support, which reduced the number of staff available to serve at security checkpoints and may hinder TSA's ability to carry out its mission. *(Transportation Security Administration Information Technology Management Progress and Challenges*, OIG-13-101)

*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. (*Transportation Security Administration Office of Inspection's Efforts To Enhance Transportation Security,* OIG-13-123)

*Airport Employee Screening*

In June of last year, we issued a report that looked at TSA's controls over the vetting of aviation workers possessing or applying for credentials that allow unescorted access to secured areas of commercial airports. We found that TSA had less effective controls in place for ensuring that aviation workers (1) had not committed crimes that would disqualify them from having unescorted access to secure airports areas, and (2) had lawful status and were authorized to work in the United States. In general, TSA relied on airport operators to perform criminal history and work authorization checks, but had limited oversight over these commercial entities. Thus, TSA lacked assurance that it properly vetted all credential applicants.

Further, thousands of records used for vetting workers contained potentially incomplete or inaccurate data, such as an initial for a first name and missing social security numbers. TSA did not have appropriate edit checks in place to reject such records from vetting. Without complete and accurate information, TSA risks credentialing and providing unescorted access to secure airport areas for workers with potential to harm the nation's air transportation system.

Finally, we noted that TSA did not have access to a complete set of records because TSA was not authorized to receive all terrorism-related information under current interagency watchlisting policy. I am pleased to report that that situation has now been remedied. (*TSA Can Improve Aviation Worker Vetting,* OIG-15-98)

*Management of Contracts*

Our audits have identified issues in the method by which TSA administers its contracts as well. This year, we released a report on TSA's management of its human capital contract, valued at about $1.2 billion over eight and a half years. We found that TSA's oversight of the HR Access contract needs improvement. Specifically, TSA has limited options for holding the contractor accountable for performance deficiencies. There were instances in which TSA

did not hold the contractor monetarily accountable for personally identifiable information (PII) violations. Had TSA consistently applied the terms and conditions of the contract, the agency could have saved approximately $4.2 million. TSA also did not hold the contractor monetarily liable for noncompliance with statement of work requirements relating to veterans' preference.

Additionally, TSA needs to improve its assessment and monitoring of contractor performance. Performance metrics are not comprehensive. TSA inflates performance evaluation scores, and those scores are not consistently affected by poor performance. Had TSA not inflated performance scores and given the contractor positive scores for work that was not completed, the agency could have saved approximately $350,000 in performance awards paid. Furthermore, TSA does not consistently conduct day-to-day independent monitoring of contractor performance. TSA's lack of contract oversight resulted in performance awards that do not accurately reflect performance. In addition, award fees, totaling $4.5 million, may not be justified, and TSA has no assurance it received the best value for its money. (*TSA's Human Capital Services Contract Terms and Oversight Need Strengthening*, OIG-16-32)

**Future Work**

We will continue to examine TSA's programs and operations and report our results. In addition to the new round of penetration testing we will be conducting this summer, we are in the process of conducting the following audits and inspections:

- An audit to determine whether TSA has policies and procedures in place to identify and address employee misconduct and misuse of Government resources in the Federal Air Marshals Service.

- An audit to 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.

- A verification review to determine whether TSA implemented recommendations from our May 2013 report, *Transportation Security Administration's Screening of Passengers by Observation Techniques*, OIG-13-91, to improve the program's effectiveness.

- Auditing whether the Federal Air Marshal Service adequately manages its resources to detect, deter, and defeat threats to the civil aviation system.

- An inspection identifying and testing selected controls over SIDA access badges issued by airport operators.

- Synthesize the results of our airport information technology 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.

Mr. Chairman, this concludes my testimony. I welcome any questions you or other members of the Committee may have.