OFFICE OF INSPECTOR GENERAL

Testimony of Inspector General John Roth

Before the Committee on Oversight and Government Reform

United States House of Representatives

"Examining Management Practices and Misconduct at TSA: Part II"

Homeland Security

May 12, 2016
9:00 AM

DHS OIG HIGHLIGHTS

Examining Management Practices and Misconduct at TSA: Part II

May 12, 2016

Why We Did This

The audits, inspections, and investigations conducted by DHS OIG are part of our ongoing efforts to ensure the efficiency and integrity of TSA. Investigations of TSA personnel make up a large portion of our overall investigative workload.

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 as well as our role in investigating TSA misconduct:

- 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 contacts; 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.

- Last year, we received 1,000 complaints from or about TSA employees and investigated about 40. Whistleblowers play an important part in identifying waste, fraud, and abuse and we have taken steps to improve our Whistleblower Protection Program.

DHS Response

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

Chairman Chaffetz, Ranking Member Cummings, and members of the Committee, thank you for inviting me to testify on management practices at TSA.

One year ago tomorrow, I testified before this Committee at a hearing on TSA's program 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."

In November of last year I testified before this Committee and stated that:

> [T]he 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.

Today, I still believe that to be true. 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 over 1.8 million passengers a day at 450 of

our Nation's airports. Complicating this responsibility is the constantly evolving threat by adversaries willing to use any means at their disposal to incite terror.

The dangers TSA must contend with are complex and not within its control. Recent media reports have indicated that some in the U.S. intelligence community warn terrorist groups like the Islamic State (ISIS) may be working to build the capability to carry out mass casualty attacks, a significant departure from – and posing a different type of threat – 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 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.

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*)

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

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

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 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*)

Last summer we engaged in covert penetration 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. The specific result of our covert testing, like the testing we have done in the past, is classified at the Secret level. However, we can 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, TSA's response to our 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. 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. Consistent with our obligations under the *Inspector General Act*, we will report our results to this Committee as well as other committees of jurisdiction.

[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.

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, 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.

- This week, 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, Advanced Imaging Technology, and Credential Authentication Technology. This program enables the remote management of this equipment by connecting it to a centralized server 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 were 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)*

OIG's Role in Investigating Misconduct at TSA

Through the *Inspector General Act of 1978* (*IG Act*), Congress established Inspectors General, in part, in response to concerns about integrity and accountability and failures of other forms of government oversight. The *IG Act* charged Inspectors General, among other tasks, with preventing and detecting fraud and abuse in agency programs and activities; conducting investigations and audits; and recommending policies to promote efficiency, economy, and effectiveness. The position of Inspector General was strengthened by provisions in the *IG Act* creating independence from department officials, providing powers of investigation and subpoena, and reporting to the Secretary as well as Congress.

Inspectors General play a critical role in ensuring transparent, honest, effective, and accountable government. The personal and organizational independence of OIG investigators, free to carry out their work without interference by agency officials, is essential to maintaining the public trust not only in OIG's work, but in the DHS workforce as a whole. The American public must fundamentally trust that government employees will be held accountable for crimes or serious misconduct by an independent fact finder.

OIG and DHS Internal Affairs Offices

DHS Management Directive (MD) 0810.1 implements the authorities of the *Inspector General Act* in DHS. MD 0810.1 establishes OIG's right of first refusal to conduct investigations of criminal misconduct by DHS employees and the right to supervise any such investigations conducted by DHS internal affairs offices. The MD requires that all allegations of criminal misconduct by DHS employees and certain other allegations received by the components—generally those against higher ranking DHS employees—be referred to OIG immediately upon receipt of the allegations.

Many DHS components, including TSA, have an internal affairs office that conducts investigations. Under the authority of the *IG Act*, OIG has oversight responsibility for those internal affairs offices. This oversight responsibility generally takes three forms.

- First, we determine upon receipt of the complaint whether the allegations are the type that should be investigated by the OIG rather than the component's internal affairs office. We have the absolute right under the *Inspector General Act* to conduct any investigation without interference. Except for a few narrow categories of matters (which must be reported to Congress), not even the Secretary can prevent the OIG from conducting an investigation.

- Second, for those investigations the internal affairs offices conduct, we have the authority to receive reports on and monitor the status of investigations.

- Lastly, we conduct oversight reviews of DHS component internal affairs offices to ensure compliance with applicable policies, reporting requirements, and accepted law enforcement practices. Our reviews are conducted on a three-year cycle and our findings are published through our website. In 2015 and the first half of 2016, we reviewed three component internal affairs offices and made 70 recommendations for improvement. Our recommendations ranged from suggestions for improving the processing of allegations to counseling a component to seek the proper investigative authority for its internal affairs office. These reviews are critical to ensuring that misconduct allegations, whistleblowers, and those reporting allegations of wrongdoing by DHS employees are treated with the seriousness they deserve.

Our investigative process generally follows these steps:

1. An allegation of misconduct is reported to OIG or other appropriate office; if reported to an office other than OIG and several criteria for seriousness are met, the component must report the allegation to OIG.

2. Whether the allegation was reported directly to OIG or through a component, OIG will decide to investigate the allegation or refer it to the component's internal affairs office; if referred, the component can decide to investigate the allegation or take no action.

3. If OIG decides to investigate, we develop sufficient evidence to substantiate or not substantiate an allegation and write a report of investigation.

4. OIG provides its investigative findings to the affected component, which uses this information to decide whether discipline is warranted. We are not involved in decisions regarding discipline after we provide our investigative findings.

5. For criminal matters, OIG presents its investigative findings to the Department of Justice (DOJ) for a determination of whether DOJ will pursue judicial action.

The Department employs more than 240,000 employees (and nearly an equal number of contract personnel), including a large number of law enforcement officers and agents in U.S Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement, the Secret Service, and the TSA. These

officers and agents protect the President, our borders, travel, trade, and financial and immigration systems. Additionally, the Department employs an equal number of contractors.

In fiscal year (FY) 2015, we received almost 18,000 complaints. A substantial number of the complaints alleged that DHS personnel engaged in misconduct. We initiated 664 investigations. The remainder were referred to component internal affairs offices, other agencies, or were administratively closed. In FY 2015, our investigations resulted in 104 criminal convictions and 37 personnel actions.

Investigations against TSA personnel comprise a portion of our overall work. In the last fiscal year, we received about 1,000 complaints either from or about TSA employees. We typically accept for investigation about 40 of those cases per year. Our criteria for case selection generally involves an assessment of the seriousness of the allegation, the rank or grade of the individual involved, and whether OIG's uniquely independent role is necessary to ensure that the case is handled appropriately.

Whistleblower Protection

We value the contributions that whistleblowers make in identifying, fraud, waste, and abuse. Federal law provides protections for employees who disclose wrongdoing. Specifically, managers are prohibited from retaliating against them by taking or threatening to take any adverse personnel actions because they report misconduct. The *IG Act* also gives us the absolute right to protect the identity of our witnesses, who we depend on to expose fraud, waste, and abuse.

DHS employees' contributions in exposing poor management practices have been well documented. In the TSA context, for example, we investigated a whistleblower's allegation that a notorious 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 initially disagreed with our recommendation regarding the Secure Flight program, but I am pleased to report has reversed its earlier opposition. (Allegation of Granting Expedited Screening through TSA PreCheck Improperly (Redacted) OIG-15-45)

When I arrived at OIG about two years ago, I was concerned about how we had been managing our Whistleblower Protection Program. I wanted to raise our profile within DHS as the entity to report fraud, waste, and abuse. My goal is to make sure we have a whistleblower program that is as good as or better than any OIG in the Federal Government. While we have made some very good efforts along those lines in the past, I decided that we need to be more proactive. To that end, I have:

- Asked a senior executive at the OIG to be the statutorily-mandated DHS Whistleblower Ombudsman. He is spearheading the efforts to ensure that all DHS personnel and contractors, in every component, understand their rights to report fraud, waste, and abuse, and to be protected from retaliation for doing so.

- Revamped the intake process for allegations of whistleblower retaliation. Now, each claim will be examined by a specially-trained group of investigators within our Whistleblower Protection Office, being assisted and supported by our lawyers in the Office of Counsel.

- Obtained, for the first time in our history, official certification from the Office of Special Counsel that our whistleblower protection program met the whistleblower protection requirements of 5 U.S.C. § 2302(c).

While I am confident that these changes are a step in the right direction, I also understand that it will take constant vigilance and continual effort to ensure that whistleblowers who have claims of retaliation are listened to and that their claims are fairly and independently investigated.

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