OFFICE OF INSPECTOR GENERAL

Testimony of Inspector General John Roth

Before the Committee on Commerce, Science, and Transportation

United States Senate

"A Look Ahead: Inspector General Recommendations for Improving Federal Agencies"

Homeland Security

February 8, 2017
10:00 AM

Chairman Thune, Ranking Member Nelson, and Members of the Committee, thank you for inviting me to testify on the work of the Office of Inspector General of the Department of Homeland Security.

As you know, DHS' mission to protect the Nation entails a wide array of responsibilities. These range from facilitating the flow of commerce and travelers, countering terrorism, and securing and managing the border to enforcing and administering immigration laws and preparing for and responding to natural disasters.

Our office reflects the size and complexity of the Department. In a typical year, we issue nearly 200 audit and inspection reports and conduct over 600 investigations. In our audit and inspection reports, we make nearly 400 recommendations in an average year. We receive nearly 19,000 complaints through our hotline and website, including over 400 whistleblower complaints per year, and have pending nearly 1,000 investigations at any one time.

Currently, as it relates to matters under this Committee's jurisdiction, we have 115 open recommendations. A full list of these recommendations is attached as appendix A. The number of open recommendations, particularly those with which the Department did not agree, has fallen precipitously. We are generally pleased with the level of responsiveness we have received from the Department, which we believe is a result of significant leadership commitment to the principles of an independent internal audit function.

Major Management Challenges Facing DHS

Homeland Security faces many challenges, and we at OIG have focused our energy on the major management and performance challenges. We have listed six:

- creating a unified department,
- employee morale and engagement,
- acquisition management,
- grants management,
- cybersecurity, and
- improving management fundamentals.[1]

Although significant progress has been made, the Department continues to face long-standing, persistent challenges overseeing and managing its homeland security mission. These challenges affect every aspect of the mission, from preventing terrorism and protecting our borders and transportation systems to enforcing our immigration laws, ensuring disaster resiliency, and securing cyberspace. The Department is continually tested to work as one

[1] *Major Management and Performance Challenges Facing the Department of Homeland Security*, OIG-17-08 (November 2016).

entity to achieve its complex mission. The key to sustaining the gains made thus far is a leadership commitment by the new Administration and continued thoughtful but vigorous oversight by this Committee and my office.

I will briefly discuss our work in the three areas under the Committee's jurisdiction: the Transportation Security Administration, the Coast Guard, and the Department's cyber responsibilities.

Transportation Security Administration

The Nature of the Threat

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

The dangers TSA must contend with are complex and not within its control. Recent media reports have indicated that some in the U.S. intelligence community warn terrorist groups like the Islamic State (ISIS) may be working to build the capability to carry out mass casualty attacks, a significant departure from – and posing a different type of threat than – simply encouraging lone wolf attacks. According to these media reports, a mass casualty attack has become more likely in part because of a fierce competition with other terrorist networks – being able to kill opponents on a large scale would allow terrorist groups such as ISIS to make a powerful showing. We believe such an act of terrorism would likely be carried out in 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 the 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 the intelligence community beforehand. Terrorism, especially suicide terrorism, depends on a cadre of newly-converted individuals who are often unknown to the intelligence community. Moreover, the threat of ISIS- or Al Qaeda-inspired actors – those with no formal ties to the

larger organizations, but who simply take inspiration from them – increase the possibilities of a terrorist actor being 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.

TSA Does Not Have a Risk-Based Security Strategy

TSA has many responsibilities beyond air travel, and is responsible, generally through the use of regulation and oversight, for surface transportation security. However, TSA focuses primarily on air transportation security and largely ignores other modes. We found that TSA does not have an intelligence-driven, risk-based security strategy to inform security and budget needs across all types of transportation. In 2011, TSA began publicizing that it uses an "intelligence-driven, risk-based approach" across all transportation modes. However, we found this not to be true. In an audit we released this past September, we reported that TSA specifically designed this approach to replace its one-size-fits-all approach to air passenger screening, but did not apply it to other transportation modes. Additionally, TSA's agency-wide risk management organizations provide little oversight of TSA's surface transportation security programs. TSA established an Executive Risk Steering Committee which was intended to create a crosscutting, risk-based strategy that would drive resource allocations across all modes. However, no entity at TSA, places much emphasis on non-air transportation modes.

As a result, TSA dedicated 80 percent of its nearly $7.4 billion FY 2015 budget to direct aviation security expenditures, and only about 2 percent to direct surface transportation expenditures. Its remaining resources were spent on support and intelligence functions. A formal process that incorporates risk into its budget formulation would help TSA ensure it best determines and prioritizes the resources necessary to fulfill its missions.[2]

As a result of a lack of focus on surface transportation, TSA's efforts in this area have been lacking. Recently, we have published two reports that identify significant weaknesses in TSA's ability to secure surface transportation modes and the Nation's maritime facilities and vessels. Specifically, we identified issues with the reliability of background checks for port workers, and passenger rail security.

With regard to surface transportation, we issued a report that found that TSA has failed to develop and implement regulations governing passenger rail

[2] *Transportation Security Administration Needs a Crosscutting Risk-Based Security Strategy* (OIG-16-134).

security required more than nine years ago. Specifically, although required to by the *Implementing Recommendations of the 9/11 Commission Act of 2007*, TSA neither identified high-risk carriers, nor issued regulations requiring those carriers to conduct vulnerability assessments and implement DHS-approved security plans. TSA also did not issue regulations that would require a railroad security training program. Furthermore, unlike aviation and maritime port workers, TSA has not developed regulations requiring security background checks for rail workers. TSA has just submitted a notice of proposed rulemaking on one rule to the federal register, but unfortunately, will not even commit to a timeline as to when they will move the other two regulations forward.[3]

We issued a second report that found that TSA is missing key internal controls in the Transportation Worker Identification Credential (TWIC) program. The background check process for TWICs includes a check for immigration-, criminal-, and terrorism-related offenses that would preclude someone from being granted unescorted access to secure facilities at seaports. Our review found that TSA did not adequately integrate the security measures intended to identify fraudulent applications into the background check process. This was the case notwithstanding the fact that a GAO report found the same problems five years ago.[4]

Checkpoint Performance

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.

Previous covert testing identified vulnerabilities in TSA's use of Advanced Imaging Technology (AIT) equipment at domestic airports. We previously engaged in covert penetration testing to evaluate the effectiveness of TSA's Automated Target Recognition software 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

[3] *TSA Oversight of National Passenger Rail System Security* (OIG-16-91).
[4] *TWIC Background Checks are Not as Reliable as They Could Be* (OIG-16-128).

past, is classified at the Secret level. However, we can describe the results as troubling and disappointing.[5]

Unfortunately, the results of this covert testing was in line with previous covert testing we had conducted, both on the AIT machines as well as on checked baggage and access to secured airport areas.[6]

I am pleased to report that in the last 18 months, TSA's response to our findings has represented a marked change from previous practice. TSA's leadership understood the gravity of our findings, and moved to revamp training, improve technology, and refine checkpoint policies and procedures in an attempt to increase checkpoint effectiveness. 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.

More importantly, the previous Administrator reemphasized the security mission of TSA to the workforce.

We are in the midst of another round of covert testing across the country. Consistent with our obligations under the *Inspector General Act*, we will report our results to this Committee as well as other committees of jurisdiction.

Expedited Screening and 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,

---

[5] *Covert Testing of TSA's Passenger Screening Technologies and Processes at Airport Security Checkpoints (Unclassified Summary* (OIG-15-150).

[6] *TSA Penetration Testing of Advanced Imaging Technology (Unclassified Summary), OIG 12-06*; *Covert Testing of Access Controls to Secured Airport Areas, OIG-12-26*; *Vulnerabilities Exist in TSA's Checked Baggage Screening Operations (Unclassified Summary), OIG-14-142.*

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 grant expedited screening to broad categories of individuals based on some questionable assumptions about relative risk based on factors unrelated to individual assessment of risk, create an unacceptable risk to aviation security. 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.[7]

Airport Employee Vetting and Access Controls to Secure Areas

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.

Federal regulations require individuals who apply for credentials to work in secure areas of commercial airports to undergo background checks. TSA and airport operators are required to perform these checks prior to granting individuals badges that allow them unescorted access to secure areas.

We found that TSA was generally effective in identifying individuals with links to terrorism. Since its inception in 2003, TSA has directed airports to deny or revoke 58 airport badges as a result of its vetting process for credential applicants and existing credential holders. In addition, TSA has implemented quality review processes for its scoring model, and has taken proactive steps based on non-obvious links to identify new terrorism suspects that it nominates to the watchlist.

Despite rigorous processes, TSA did not identify 73 individuals with links to terrorism because TSA is not cleared to receive all terrorism categories under current interagency watchlisting guidance. At our request, the National Counterterrorism Center (NCTC) performed 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, the interagency policy in effect at the time prevented the agency from receiving all terrorism-related codes during vetting.

[7] *Use of Risk Assessment within Secure Flight*, OIG-14-153 (June 2015).

TSA officials recognized 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. In response to this audit, the Department worked with the Intelligence Community to ensure that TSA had access to the entire TIDE. This has closed a significant vulnerability, and we are pleased to report that we were able to close our recommendation.

Additionally, this same audit found that TSA also did not have an adequate monitoring process in place to ensure that airport operators properly adjudicated credential applicants' criminal histories, and also found weaknesses in the verification process for an individual's authorization to work in the United States. Weaknesses in these programs present a security risk to aviation transportation.

TSA's Office of Security Operations performed annual inspections of commercial airport security operations, including reviews of the documentation that aviation workers submitted when applying for credentials. However, due to workload at larger airports, this inspection process looked at as few as one percent of all aviation workers' applications. In addition, we found other weaknesses in the method by which the documentation was verified.[8]

The necessity to permit access to secure areas to only known and trusted individuals should be self-evident. Those with unsupervised, unescorted access to aircraft could secrete dangerous items on board. Unfortunately, the current system has much to be desired. Open source reporting shows that those with unescorted access regularly stow contraband on airplanes. Last week, for example, American Airlines accidentally discovered during routine maintenance 31 pounds of cocaine secreted in the nose of an American Airlines Boeing 757. According to published news reports, this was the second time in three years this had occurred.[9]

Other open source media, as well as congressional hearings, have highlighted the risks involved. In 2013, an avionics technician with unescorted access to airplanes was convicted for his part in a plot to wage violent jihad by driving a bomb-laden van onto the tarmac at the Wichita airport and detonate it. His

---

[8] *TSA Can Improve Aviation Worker Vetting*, OIG-15-98 (June 2015).

[9] http://www.upi.com/Top_News/US/2017/01/31/Thirty-pounds-of-cocaine-found-in-nose-of-American-Airlines-plane/9461485853935/. This is a fairly common occurrence. See, e.g., https://www.cbp.gov/newsroom/local-media-release/cbp-jfk-seizes-cocaine-and-heroin-inside-aircraft (cocaine and heroin found in two separate incidents at JFK in 2015; secreted inside aircraft panels); http://www.actionnewsjax.com/news/local/3-kilos-of-cocaine-found-on-jetblue-plane-months-after-flight-attendant-caught-smuggling/412777000 (three kilograms of cocaine discovered on JetBlue aircraft inside wing panel in June 2016).

goal, according to the prosecutors involved in the case, was to inflict maximum casualties just before Christmas.[10] In another instance, a gun-smuggling conspiracy used a baggage handler to smuggle weapons, including loaded weapons, onto flights from Atlanta to New York. Law enforcement authorities were able to confirm that they had shipped approximately 129 firearms in that manner.[11]

Airport workers are subject to only minimal vetting – the same level of vetting, for example, that a PreCheck passenger receives – including a fingerprint-based criminal history check to determine whether an individual has been convicted of or is under indictment for certain enumerated felonies, and whether that person is on the terrorist watch list.[12] The risk presented by such limited vetting is compounded by the fact that airport workers are subject to physical screening at only two of the approximately 450 airports under TSA's jurisdiction. We believe that this creates a significant risk to aviation security.

Additionally, there is a significant risk that lost or stolen airport access badges could allow unauthorized people access to secure airport areas. In response to congressional concerns and media reports, we conducted a review of TSA's controls over access badges. Based on its comprehensive and targeted inspections, TSA has asserted that most airports adequately control badges for employees working in nonpublic areas. However, we found this not to be accurate.

From TSA's own testing conducted in 2015, as well as our own testing recently conducted, we conclude that airports do not always properly account for access media badges after they are issued to employees. TSA's current inspection practice of relying on information reported by airports about access media badges limits its oversight of badge controls. During our inspection, we found that a significant percentage of the airports we looked at did not have accurate information about active access media badges.

By testing more controls, which are designed to curtail the number of unaccounted for badges, TSA could strengthen its oversight of airports. Improved oversight by TSA, including encouraging wider use of airports' best practices, would help mitigate the risks to airport security posed by unaccounted for employee badges.[13]

---

[10] https://www.justice.gov/opa/pr/kansas-man-pleads-guilty-plot-explode-car-bomb-airport.
[11] https://www.justice.gov/usao-ndga/pr/baggage-handler-hartsfield-jackson-airport-arrested-smuggling-guns-airport-evading
[12] The felonies are listed at 49 CFR 1542.209.
[13] *TSA Could Improve Its Oversight of Airport Controls over Access Media Badges*, OIG-17-04 (October 2016).

TSA Business Practices

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

Last May, 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.[14]

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

[14] *IT Management Challenges Continue in TSA's Security Technology Integrated Program*, OIG-16-87 (May 2016).

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.[15]

Sensitive Security Information

I remain concerned about TSA's use of the Sensitive Security Information (SSI) designation. In our latest report on airport-based IT systems, TSA had demanded the redaction of information that had previously been freely published without objection, and which my IT security experts state poses no threat to aviation security. TSA's history of abusing the SSI designation is well documented, and we are conducting a review of TSA's management and use of the SSI designation, which should be out this summer. Inconsistently and inappropriately marking information in our reports as SSI impedes our ability to issue reports to the public that are transparent without unduly restricting information, which is key to accomplishing our mission and required under the *Inspector General Act*.

Coast Guard

Within the Department of Homeland Security, U.S. Customs and Border Protection's (CBP) Air and Marine Operations (AMO) and the United States Coast Guard (Coast Guard) share responsibility for maritime security missions. At the request of Congress, we reviewed the maritime missions and responsibilities of AMO and the Coast Guard.

We found that the maritime missions and responsibilities of AMO and the Coast Guard are not duplicative. Their efforts to interdict drugs and people bolster the overall effectiveness of DHS' maritime border security. The agencies contribute to the national strategy of layered maritime security and conduct different activities, which leads to more interdictions. We also found very little overlap in mission locations. For example, of the 206 combined locations where AMO and the Coast Guard conduct operations in customs waters, only 17 of them (8 percent) have similar capabilities and an overlapping area of responsibility.

However, AMO and the Coast Guard could improve coordination and communication at those 17 areas. For example, we found that the majority of

[15] *The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program*, OIG-15-86 (May 2016).

those locations did not train together, and nearly half (45%) did not coordinate operations or activities.[16]

We also supervised the annual financial statement audit, which concluded that, as it relates to the internal control environment, the Coast Guard had a number of internal control deficiencies in the areas of financial disclosure reports; accounts receivable; civilian and military payroll; financial reporting process; and accounts payable accrual. However, these deficiencies were not considered significant, and thus were not reported in the agency's FY 2015 financial statement report.[17] The FY 2016 review is ongoing.

With regard to Coast Guard's information technology issues, however, the financial statement auditors found that there were IT control deficiencies related to access controls, segregation of duties, and configuration management of Coast Guard's core financial and feeder systems. In many cases, new control deficiencies reflected weaknesses over controls and systems that were new to the scope of the FY 2015 audit. Such deficiencies limited Coast Guard's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. These issues, when combined with other IT issues, contributed to a material weakness in IT controls and financial system functionality at the DHS Department-wide level.[18]

The conclusions reached in that audit are similar to the deficiencies in the Coast Guard IT systems we discovered during our 2015 *Federal Information Security Modernization Act* (FISMA) audit. For example, we found that the Coast Guard was operating 35 separate information systems without an "Authority to Operate." This represents 56% of Coast Guard's high-value assets and mission essential systems, and 67% of all other systems. A system operating without an authority to operate means the Coast Guard cannot ensure they have implemented effective controls to protect the sensitive information stored and processed by these systems.[19] Coast Guard made significant strides in this area between our FY 2015 and FY 2016 FISMA audits, and in our latest review, had reduced the number of systems without an authority to operate to six.[20]

On a positive note, we conducted a review of the Coast Guard's major acquisition process. We did so as a result of concerns we had raised in an

---

[16] *AMO and Coast Guard Maritime Missions Are Not Duplicative, But Could Improve with Bettter Coordination*, OIG-17-03 (October 2016).
[17] *United States Coast Guard's Management Letter for DHS' FY 2015 Financial Statements Audit*, OIG-16-77.
[18] *Information Technology Management Letter for the United States Coast Guard Component of the FY 2015 Department of Homeland Security Financial Statement Audit*, OIG-16-44.
[19] *Evaluation of DHS' Information Security Program for Fiscal Year 2015*, OIG-16-08.
[20] *Evaluation of DHS' Information Security Program for Fiscal Year 2016*, OIG-17-24.

earlier 2012 audit, which found that the Coast Guard's schedule-driven acquisition process allowed the construction of Sentinel Class Fast Response Cutter to begin before all of the operational, design and technical risks were resolved. This necessitated modification of the cutters under construction, causing scheduling delays and additional costs. In this verification review, we examined the Coast Guard's acquisition of a different vessel, the Offshore Patrol Cutter, to see if the Coast Guard had absorbed the lessons from our audit. We found that the Coast Guard's plans to reduce risks during this acquisition show progress toward achieving the intended results of our earlier audit. However, it is too early in the acquisition to determine whether the Coast Guard has fully implemented its plans. We will continue to look at the issue.[21]

Cybersecurity Threat Issues

Our office looked at a number of cyber issues as it relates to DHS in the recent past.

FISMA

The *Federal Information Security Modernization Act* (FISMA) requires Federal agencies to establish security protections for information systems that support their operations and report annually on the effectiveness of information security policies, procedures, and practices. FISMA also requires that the agency OIG perform an annual independent evaluation of the agency's information security program and practices and report on agency compliance in the following areas:

1. Continuous Monitoring Management
2. Configuration Management
3. Identity and Access Management
4. Incident Response and Reporting
5. Risk Management
6. Security Training
7. Plan of Action and Milestones
8. Remote Access Management
9. Contingency Planning
10. Contractor Systems

Each year the OIG is required to issue two FISMA reports: A general FISMA report concerning the Department's "Sensitive But Unclassified," "Secret," and

[21] *Verification Review of U.S. Coast Guard's Acquisition of the Sentinel Class-Fast Response Cutter,* OIG-12-68.

"Top Secret" systems to the Office of Management and Budget; and a second report based on our assessment of DHS' intelligence systems to the Intelligence Community Inspector General (IC IG) with no recommendations. Based on the results in our IC IG report, we issue a third report to the Department that includes recommendations for correcting the deficiencies identified regarding DHS' intelligence systems.

General FISMA

For FY 2016, we found that DHS has taken actions to strengthen its information security program.[22]

On July 22, 2015, in response to cyber-attacks on the Federal Government, the DHS senior leadership ordered DHS and its Components to strengthen their cyber defenses. Components were to implement the following cybersecurity infrastructure measures within 30 days:

- consolidate all of DHS' internet traffic behind the Department's trusted internet connections,
- implement strong authentication through the use of personal identity verification (PIV) cards for all privileged and unprivileged access accounts,
- achieve 100 percent SA compliance for systems identified by the Component as high value assets and 95 percent compliance for the remaining systems, and
- retire all discontinued operating systems and servers (e.g., Windows XP and Windows Server 2000/2003).

To further enhance the Department's cyber defense, in January 2016 DHS senior leadership further ordered Components to take the following actions to protect their networks and educate their employees within 45 days:

- establish the capability to perform searches for compromise indicators within 24 hours of detected suspicious network activity,
- remove users' administrative privileges on workstations connected to the networks, and
- require two-factor authentication for all users accessing the Department's Homeland Secure Data Network.

The Components have made significant progress in remediating security weaknesses identified, compared to the same period last year. Further, as of

[22] *Evaluation of DHS' Information Security Program for Fiscal Year 2016*, OIG-17-24

May 2016, all Components were reporting information security metrics to the Department, enabling DHS to better evaluate its security posture.

Despite the progress made, Components were not consistently following DHS' policies and procedures to maintain current or complete information on remediating security weaknesses in a timely fashion. Components operated 79 unclassified systems with expired authorities to operate. Further, Components had not consolidated all internet traffic behind the Department's trusted internet connections and continued to use unsupported operating systems that may expose DHS data to unnecessary risks. We also identified deficiencies related to configuration management and continuous monitoring. Without addressing these deficiencies, the Department cannot ensure that its systems are adequately secured to protect the sensitive information stored and processed in them.

Intelligence FISMA

Pursuant to FISMA, we reviewed the Department's policies, procedures, and system security controls for the enterprise-wide intelligence system in September of last year. Since our FY 2015 evaluation, the Office of Intelligence and Analysis has continued to provide effective oversight of the department-wide system and has implemented programs to monitor ongoing security practices. In addition, Intelligence and Analysis has relocated its intelligence system to a DHS data center to improve network resiliency and support.

The Coast Guard has migrated all of its sites that process Top Secret/Sensitive Compartmented Information to the Department of Defense Intelligence Information System owned by the Defense Intelligence Agency. However, Coast Guard must continue to work with the Defense Intelligence Agency to clearly identify agency oversight responsibilities for the Department of Defense Intelligence Information System enclaves that support Coast Guard's intelligence operations.[23]

Science and Technology Directorate Insider Threats

The DHS Science and Technology Directorate (S&T) is the primary DHS research arm. Its mission is to strengthen the nation's security and resiliency by providing knowledge products and innovative solutions for DHS. Trusted insiders at S&T are given elevated access to mission-critical assets, including personnel, facilities, information, equipment, networks, and systems. Trusted insiders may also be aware of weaknesses in organizational policies and

[23] *Review of DHS' Information Security Program for Intelligence Systems of Fiscal Year 2016,* OIG-16-131 (September 2016).

procedures, as well as physical and technical vulnerabilities in computer networks and information systems.

We have begun an audit to assess the effectiveness of steps S&T has taken to protect its IT assets and data from potential unauthorized access, disclosure, or misuse by its employees, contractors, and business partners—especially those with special or elevated access based upon their job descriptions or functions. The scope of our review includes S&T headquarters and selected S&T locations that use or maintain IT systems and data; security operations and incident response centers; and other locations as needed. We expect to complete this performance audit and report on the results in February 2017.

Mr. Chairman, this concludes my testimony. I am happy to answer any questions you or any members of the committee may have.

Department of Homeland Security Open Recommendations as of December 31, 2016 (TSA, USCG, FISMA)								
	Report No.	**Report Title**	**Date Issued**	**Recommendation**	**Rec. No.**	**DHS Comp.**	**Questioned Cost (Federal Share)**	**Funds to be Put to Better Use (Federal Share)**
1	OIG-15-16	Evaluation of DHS' Information Security Program for Fiscal Year 2014	12/12/2014	We recommend that the Chief Information Security Officer (CISO) evaluate whether the Department's system inventory methodology is effective to prevent Components from circumventing the existing process to procure or develop new systems.	2	MGMT		
2	OIG-15-16	Evaluation of DHS' Information Security Program for Fiscal Year 2014	12/12/2014	We recommend that the CISO strengthen the process to ensure that all DHS systems receive the proper authority to operate in accordance with applicable OMB and National Institute of Standards and Technology (NIST) security authorization guidance.	6	MGMT		
3	OIG-16-08	Evaluation of DHS' Information Security Program for Fiscal Year 2015	11/13/2015	We recommend that the DHS CISO strengthen the Department's oversight of the Component's information security programs to ensure they comply with requirements throughout the year instead of peaking in compliance during the months leading up to annual *Federal Information Security Management Act of 2002, as amended* (FISMA) reporting.	3	MGMT		
4	OIG-16-08	Evaluation of DHS' Information Security Program for Fiscal Year 2015	11/13/2015	We recommend that DHS CISO implement input validation controls on DHS' enterprise management systems and perform quality reviews to validate that the information entered is accurate.	5	MGMT		
5	OIG-12-26	Transportation Security Administration Covert Testing of Access Controls to Secured Airport Areas	1/6/2012	This is a classified report.	5	TSA		
6	OIG-14-132	Audit of Security Controls for DHS Information Technology Systems at Dallas/Fort Worth International Airport	9/5/2014	We recommend that the TSA Chief Information Officer (CIO) establish a process to report Security Technology Integrated Program (STIP) computer security incidents to TSA Security Operations Center (SOC).	3	TSA		
7	OIG-14-132	Audit of Security Controls for DHS Information Technology Systems at Dallas/Fort Worth International Airport	9/5/2014	We recommend that the TSA Chief Information Officer (CIO) provide required vulnerability assessment reports to the DHS Vulnerability Management Branch.	5	TSA		
8	OIG-14-142	(U) Vulnerabilities Exist in TSA's Checked Baggage Screening Operations	9/16/2014	This is a classified report.	4	TSA		

	Report No.	Report Title	Date Issued	Recommendation	Rec. No.	DHS Comp.	Questioned Cost (Federal Share)	Funds to be Put to Better Use (Federal Share)
9	OIG-14-142	(U) Vulnerabilities Exist in TSA's Checked Baggage Screening Operations	9/16/2014	This is a classified report.	5	TSA		
10	OIG-14-153	Use of Risk Assessment within Secure Flight	9/9/2014	(SSI) This recommendations contains Sensitive Security Information.	1	TSA		
11	OIG-15-18	Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport-Sensitive Security Information	12/16/2014	We recommend that the TSA CIO designate the intrusion detection and surveillance Security Systems as DHS information technology (IT) systems and implement applicable management, technical, operational, and privacy controls and reviews.	6	TSA		
12	OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	(SSI) This recommendations contains Sensitive Security Information.	1	TSA		
13	OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	(SSI) This recommendations contains Sensitive Security Information.	2	TSA		
14	OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	(SSI) This recommendations contains Sensitive Security Information.	4	TSA		
15	OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	(SSI) This recommendations contains Sensitive Security Information.	5	TSA		
16	OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	(SSI) This recommendations contains Sensitive Security Information.	9	TSA		
17	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.	10	TSA		
18	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.	13	TSA		
19	OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	(SSI) This recommendations contains Sensitive Security Information.	14	TSA		

	Report No.	Report Title	Date Issued	Recommendation	Rec. No.	DHS Comp.	Questioned Cost (Federal Share)	Funds to be Put to Better Use (Federal Share)
20	OIG-15-45	Allegations of Granting Expedited Screening through TSA PreCheck Improperly (OSC File No. DI-14-3679)	3/16/2015	(SSI) This recommendations contains Sensitive Security Information.	1	TSA		
21	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 (OSC) 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.	1	TSA		
22	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.	2	TSA		
23	OIG-15-88	Audit of Security Controls for DHS Information Technology Systems at San Francisco International Airport	5/7/2015	We recommend that the TSA CIO provide required vulnerability assessment reports to the DHS Vulnerability Management Branch for STIP servers tested, similar to those operating at San Francisco International Airport (SFO).	14	TSA		
24	OIG-15-88	Audit of Security Controls for DHS Information Technology Systems at San Francisco International Airport	5/7/2015	We recommend that the TSA CIO update the operating systems on STIP servers to a vendor-supported version that can be patched to address emerging vulnerabilities.	15	TSA		
25	OIG-15-98	TSA Can Improve Aviation Worker Vetting	6/4/2015	We recommend that the TSA Acting Administrator 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.	6	TSA		

	Report No.	Report Title	Date Issued	Recommendation	Rec. No.	DHS Comp.	Questioned Cost (Federal Share)	Funds to be Put to Better Use (Federal Share)
26	OIG-15-118	Transportation Security Administration's Management of Its Federal Employees' Compensation Act Program	8/6/2015	We recommend that the Assistant Administrator, Office of Human Capital for TSA and the Federal Air Marshal Service conduct a cost-benefit analysis to ensure all costs are considered to implement one medical case management system for TSA, including its Federal Air Marshal Service.	2	TSA		
27	OIG-16-32	TSA's Human Capital Services Contract Terms and Oversight Need Strengthening	1/29/2016	We recommend that TSA's Assistant Administrator for the Office of Acquisition ensure that Personnel Futures Program (PFP) contracts contain lessons learned from the human capital services (HR Access) contract that include: - developing and implementing policy guidance for administering award fee type contracts; - monetary penalties for performance deficiencies including violating Federal law; - performance timeframes and prescriptive language in the statement of works (SOW); - performance metrics that correspond to the majority of sections in the SOWs; - timeframes for correcting performance deficiencies; and - requirements for initiating and issuing performance letters, and for factoring performance deficiencies addressed in those letters into performance evaluations and award determinations.	1	TSA		
28	OIG-16-87	IT Management Challenges Continue in TSA's Security Technology Integrated Program	5/10/2016	We recommend that the TSA CIO and Assistant Administrator for OSC jointly ensure that IT security controls are included in STIP system design and implementation so that STIP servers are not deployed with known technical vulnerabilities.	1	TSA		
29	OIG-16-87	IT Management Challenges Continue in TSA's Security Technology Integrated Program	5/10/2016	We recommend that the TSA CIO and Assistant Administrator for OSC jointly ensure that STIP servers use approved operating systems for which the Department has established minimum security baseline configuration guidance.	2	TSA		
30	OIG-16-87	IT Management Challenges Continue in TSA's Security Technology Integrated Program	5/10/2016	We recommend that the TSA CIO and Assistant Administrator for the Office of Security Capabilities jointly ensure that STIP servers have the latest software patches installed so that identified vulnerabilities will not be exploited.	3	TSA		

	Report No.	Report Title	Date Issued	Recommendation	Rec. No.	DHS Comp.	Questioned Cost (Federal Share)	Funds to be Put to Better Use (Federal Share)
31	OIG-16-87	IT Management Challenges Continue in TSA's Security Technology Integrated Program	5/10/2016	We recommend that the TSA CIO and Assistant Administrator for OSC jointly ensure that IT security testing is performed so that STIP servers are not deployed with known technical vulnerabilities.	4	TSA		
32	OIG-16-87	IT Management Challenges Continue in TSA's Security Technology Integrated Program	5/10/2016	We recommend that the TSA CIO and Assistant Administrator for OSC jointly ensure that authorized TSA staff obtain and change administrator passwords for all STIP servers at airports so that contractors no longer have full control over this equipment at airports.	5	TSA		
33	OIG-16-87	IT Management Challenges Continue in TSA's Security Technology Integrated Program	5/10/2016	We recommend that the TSA CIO and Assistant Administrator for OSC jointly implement a contractor oversight process so that only authorized and approved software, along with timely updates, is installed on STIP airport servers.	6	TSA		
34	OIG-16-87	IT Management Challenges Continue in TSA's Security Technology Integrated Program	5/10/2016	We recommend that the TSA CIO and Assistant Administrator for OSC jointly inventory all locations at Orlando International Airport housing STIP servers and switches and ensure that these locations comply with DHS policy concerning physical security controls.	7	TSA		
35	OIG-16-87	IT Management Challenges Continue in TSA's Security Technology Integrated Program	5/10/2016	We recommend that the TSA CIO and Assistant Administrator for OSC jointly ensure an adequate operational recovery capability for STIP servers at Data Center 1 (DC1) in case Data Center 2 (DC2) becomes inaccessible.	8	TSA		
36	OIG-16-87	IT Management Challenges Continue in TSA's Security Technology Integrated Program	5/10/2016	We recommend that the TSA CIO and Assistant Administrator for OSC jointly establish a process for providing STIP server vulnerability assessment reports to the Department so that DHS leadership may adequately monitor system compliance capability.	9	TSA		
37	OIG-16-87	IT Management Challenges Continue in TSA's Security Technology Integrated Program	5/10/2016	We recommend that the TSA CIO and Assistant Administrator for OSC jointly ensure that IT security requirements are included in equipment procurement contracts for IT components of STIP and passenger and checked baggage screening equipment as required.	10	TSA		

	Report No.	Report Title	Date Issued	Recommendation	Rec. No.	DHS Comp.	Questioned Cost (Federal Share)	Funds to be Put to Better Use (Federal Share)
38	OIG-16-87	IT Management Challenges Continue in TSA's Security Technology Integrated Program	5/10/2016	We recommend that the TSA CIO and Assistant Administrator for OSC jointly institute controls so that all IT costs associated with STIP are accurately captured and reported in annual budget submissions as required.	11	TSA		
39	OIG-16-91	TSA Oversight of National Passenger Rail System Security	5/13/2016	We recommend that the TSA Administrator ensure TSA develops and adheres to a detailed, formal milestone plan to deliver the remaining 9/11 Act Notices of Proposed Rulemaking to DHS.	1	TSA		
40	OIG-16-128	TWIC Background Checks are Not as Reliable as They Could Be	9/1/2016	We recommend that the Assistant Administrator, Office of Intelligence and Analysis, Transportation Security Administration conduct a comprehensive risk analysis of the Security Threat Assessment processes to identify areas needing additional internal controls and quality assurance procedures; and develop and implement those procedures, including periodic reviews to evaluate their effectiveness.	2	TSA		
41	OIG-16-128	TWIC Background Checks are Not as Reliable as They Could Be	9/1/2016	We recommend that the Assistant Administrator, Office of Intelligence and Analysis, Transportation Security Administration improve Transportation Worker Identification Credential program-level performance metrics to ensure they align with the program's core objectives, and direct management officials to use these metrics for all the supporting offices.	3	TSA		
42	OIG-16-128	TWIC Background Checks are Not as Reliable as They Could Be	9/1/2016	We recommend that the Assistant Administrator, Office of Intelligence and Analysis, Transportation Security Administration review current Transportation Worker Identification Credential Security Threat Assessment guidance to ensure it provides adjudicators the necessary information and authority to complete Security Threat Assessments.	4	TSA		

	Report No.	Report Title	Date Issued	Recommendation	Rec. No.	DHS Comp.	Questioned Cost (Federal Share)	Funds to be Put to Better Use (Federal Share)
43	OIG-16-134	TSA Needs a Crosscutting Risk-Based Security Strategy	9/9/2016	We recommend that the Deputy Administrator, TSA, develop and implement a crosscutting risk-based security strategy that encompasses all transportation modes. The strategy should, at a minimum: - define intelligence-driven, risk-based security; - identify objectives for an intelligence-driven, risk-based security approach; - identify steps for all transportation modes to achieve risk-based security objectives; - provide guidelines for aligning resources with risk; - establish priorities, milestones, and performance measures to gauge the effectiveness of the strategy; and - establish responsible parties and timelines for strategy implementation.	1	TSA		
44	OIG-16-134	TSA Needs a Crosscutting Risk-Based Security Strategy	9/9/2016	We recommend that the Deputy Administrator, TSA, establish a formal budget planning process that uses risk to help inform resource allocations.	3	TSA		
45	OIG-17-04	TSA Could Improve Its Oversight of Airport Controls over Access Media Badges	10/14/2016	We recommend that the TSA Administrator: Direct TSA personnel to conduct additional tests of access media badge controls during comprehensive and targeted inspections of U.S. airports.	1	TSA		
46	OIG-17-04	TSA Could Improve Its Oversight of Airport Controls over Access Media Badges	10/14/2016	We recommend that the TSA Administrator: Issue guidance to U.S. airports clearly explaining how to determine whether an airport's lost, stolen, and unaccounted for access media badges are exceeding the 5 percent threshold.	2	TSA		
47	OIG-17-04	TSA Could Improve Its Oversight of Airport Controls over Access Media Badges	10/14/2016	We recommend that TSA share with airport operators the best practices some airports use to mitigate the risks of lost, stolen, and unaccounted for access media badges and encourage airport operators to use these practices when feasible.	3	TSA		
48	OIG-17-14	Summary Report on Audits of Security Controls for TSA Information Technology Systems at Airports	11/29/2016	We recommend that the TSA CIO update TSA's Business Impact Analyses for TSA Network (TSANet) and Security Technology Integrated Program (STIP) to include the TSA local area networks (LAN), points of contact, and business processes that would be adversely affected by a potential communications outage at airports.	1	TSA		

	Report No.	Report Title	Date Issued	Recommendation	Rec. No.	DHS Comp.	Questioned Cost (Federal Share)	Funds to be Put to Better Use (Federal Share)
49	OIG-17-14	Summary Report on Audits of Security Controls for TSA Information Technology Systems at Airports	11/29/2016	We recommend that the TSA CIO establish a plan to conduct recurring reviews of the operational, technical, and management security controls for TSA IT systems at U.S. airports nationwide.	2	TSA		
50	OIG-10-11	Independent Auditors' Report on DHS' FY 2009 Financial Statements and Internal Control Over Financial Reporting	11/13/2009	We recommend that the Coast Guard implement accounting and financial reporting processes including an integrated general ledger system that is *The Federal Financial Managers Improvement Act of 1996* (FFMIA) compliant.	I-A.4	USCG		
51	OIG-10-11	Independent Auditors' Report on DHS' FY 2009 Financial Statements and Internal Control Over Financial Reporting	11/13/2009	We recommend that the Coast Guard design and implement policies, procedures, and internal controls to support the completeness, existence, accuracy, and presentation and disclosure assertions related to the data utilized in developing disclosure and related supplementary information for Stewardship property, plant, and equipment (PP&E) that is consistent with generally accepted accounting principles (GAAP).	I-D.8	USCG		
52	OIG-11-86	U.S. Coast Guard's Marine Safety Program – Offshore Vessel Inspections	6/1/2011	We recommend that the Assistant Commandant for Marine Safety, Security and Stewardship, U.S. Coast Guard complete and disseminate to field units New Construction Project Inspector Performance Qualification Standards and update the Marine Safety Manual accordingly.	1	USCG		
53	OIG-11-86	U.S. Coast Guard's Marine Safety Program – Offshore Vessel Inspections	6/1/2011	We recommend that the Assistant Commandant for Marine Safety, Security and Stewardship, U.S. Coast Guard augment Marine Information for Safety and Law Enforcement (MISLE) access controls, and develop subsequent policy, so that the same person cannot open, complete, and close an inspection case.	3	USCG		
54	OIG-12-07	Independent Auditors' Report on DHS' FY 2011 Integrated Financial Statements and Internal Control over Financial Reporting	11/11/2011	We recommend that the Coast Guard, establish new or improve existing policies, procedures, and related internal controls to ensure that: The year-end close-out process, reconciliations, and financial data and account analysis procedures are supported by documentation, including evidence of effective management review and approval, and beginning balances in the following year are determined to be reliable and auditable.	I.A.3.a	USCG		

	Report No.	Report Title	Date Issued	Recommendation	Rec. No.	DHS Comp.	Questioned Cost (Federal Share)	Funds to be Put to Better Use (Federal Share)
55	OIG-12-07	Independent Auditors' Report on DHS' FY 2011 Integrated Financial Statements and Internal Control over Financial Reporting	11/11/2011	We recommend that the Coast Guard, establish new or improve existing policies, procedures, and related internal controls to ensure that: All intra-governmental activities and balances are reconciled on a timely basis, accurately reflected in the financial statements, and differences are resolved in a timely manner in coordination with the Department's Office of Financial Management (OFM).	I.A.3.e	USCG		
56	OIG-13-20	Independent Auditors' Report on DHS FY 2012 Consolidated Financial Statements and Report on Internal Control Over Financial Reporting	11/14/2012	We recommend that the Coast Guard establish new or improve existing policies, procedures, and related internal controls to ensure that: All non-standard adjustments (i.e., journal entries, top side adjustments, and scripts) impacting the general ledger are adequately researched, supported, and reviewed prior to their recording in the general ledger.	I.A.1.c.i	USCG		
57	OIG-13-20	Independent Auditors' Report on DHS FY 2012 Consolidated Financial Statements and Report on Internal Control Over Financial Reporting	11/14/2012	We recommend that the Coast Guard establish new or improve existing policies, procedures, and related internal controls to ensure that: All non-GAAP policies are identified and their quantitative and qualitative financial statement impacts have been documented.	I.A.1.c.ii	USCG		
58	OIG-13-20	Independent Auditors' Report on DHS FY 2012 Consolidated Financial Statements and Report on Internal Control Over Financial Reporting	11/14/2012	We recommend that the Coast Guard: Continue to improve the enforcement of existing policies and procedures related to processing obligation transactions and the periodic review and validation of undelivered orders. In particular, emphasize the importance of performing effective reviews of open obligations, obtaining proper approvals, and retaining supporting documentation.	I.E.1.a	USCG		
59	OIG-13-20	Independent Auditors' Report on DHS FY 2012 Consolidated Financial Statements and Report on Internal Control Over Financial Reporting	11/14/2012	We recommend that the Coast Guard: Continue with current remediation efforts to develop and implement policies, procedures, and internal controls over the monitoring of reimbursable agreements and unfilled customer orders to ensure activity, including closeout and de-obligation, is recorded timely and accurately.	I.E.1.b	USCG		

	Report No.	Report Title	Date Issued	Recommendation	Rec. No.	DHS Comp.	Questioned Cost (Federal Share)	Funds to be Put to Better Use (Federal Share)
60	OIG-13-20	Independent Auditors' Report on DHS FY 2012 Consolidated Financial Statements and Report on Internal Control Over Financial Reporting	11/14/2012	We recommend that the Coast Guard: Implement sufficient policies and procedures for recording the appropriate budgetary entries timely upon receipt of goods, and prior to payment.	I.E.1.c	USCG		
61	OIG-13-19	Identification, Reutilization, and Disposal of Excess Personal Property by the United States Coast Guard	12/21/2012	We recommend that the Assistant Commandant for Resources and Chief Financial Officer (CFO) develop and implement a demilitarization program, in coordination with the Department of Defense Demilitarization Office, that includes training and certification for United States Coast Guard personnel who manage, oversee, or process personal property from acquisition to disposal.	3	USCG		
62	OIG-13-19	Identification, Reutilization, and Disposal of Excess Personal Property by the United States Coast Guard	12/21/2012	We recommend that the Assistant Commandant for Resources and CFO develop and implement a process to enter and track all classified personal property in the Oracle Fixed Asset Module. Develop and implement standardized policies and procedures to ensure accountability, monitoring, and oversight of disposal of classified personal property components (e.g., hard drives and printer cartridges).	4	USCG		
63	OIG-13-19	Identification, Reutilization, and Disposal of Excess Personal Property by the United States Coast Guard	12/21/2012	We recommend that the Assistant Commandant for Resources and CFO develop and implement a comprehensive training program, to include reutilization and disposal, for property managers, tailored to each level of personal property management responsibility. The training should include Commanding Officers, Accountable Property Officers, Personal Property Administrators, and Property Custodians and mandatory training for Oracle Fixed Asset Module users before granting future access.	6	USCG		

	Report No.	Report Title	Date Issued	Recommendation	Rec. No.	DHS Comp.	Questioned Cost (Federal Share)	Funds to be Put to Better Use (Federal Share)
64	OIG-13-19	Identification, Reutilization, and Disposal of Excess Personal Property by the United States Coast Guard	12/21/2012	We recommend that the Assistant Commandant for Resources and CFO develop and implement policies and procedures to account for newly purchased computers that comply with the U.S. Coast Guard's Personal Property Management Manual requirement for entry of personal property into the Oracle Fixed Asset Module within 30 calendar days of receipt from the vendor.	7	USCG		
65	OIG-13-92	Marine Accident Reporting, Investigations, and Enforcement in the United States Coast Guard	5/23/2013	We recommend that the USCG Assistant Commandant for Resources and CFO implement an investigations and inspections retention plan to ensure qualified personnel are retained within the inspections and investigations specialties.	1	USCG		
66	OIG-13-92	Marine Accident Reporting, Investigations, and Enforcement in the United States Coast Guard	5/23/2013	We recommend that the USCG Assistant Commandant for Resources and CFO revise and strengthen its personnel management policies by implementing provisions of the 2010 Coast Guard Authorization Act, which allows promotions by specialty for marine inspectors and investigators to foster retention and continuity.	2	USCG		
67	OIG-13-92	Marine Accident Reporting, Investigations, and Enforcement in the United States Coast Guard	5/23/2013	We recommend that the USCG Assistant Commandant for Resources and CFO develop a complete process with sufficient resources to review, track, and address all recommendations resulting from investigations reports.	3	USCG		
68	OIG-13-92	Marine Accident Reporting, Investigations, and Enforcement in the United States Coast Guard	5/23/2013	We recommend that the USCG Assistant Commandant for Resources and CFO provide training and guidance to all investigations personnel on all enforcement options.	5	USCG		
69	OIG-13-92	Marine Accident Reporting, Investigations, and Enforcement in the United States Coast Guard	5/23/2013	We recommend that the USCG Assistant Commandant for Resources and Chief Financial Officer develop Civil Penalty enforcement training guidelines for preparing and supporting Civil Penalty cases for all investigations staff. USCG should consider using officers with previous experience in the Hearing Office to complete this task.	6	USCG		

	Report No.	Report Title	Date Issued	Recommendation	Rec. No.	DHS Comp.	Questioned Cost (Federal Share)	Funds to be Put to Better Use (Federal Share)
70	OIG-14-18	Independent Auditors' Report on DHS' FY 2013 Financial Statements and Internal Control over Financial Reporting	12/11/2013	We recommend that Coast Guard: Fully adhere to established inventory policies and procedures.	C.1.b	USCG		
71	OIG-14-18	Independent Auditors' Report on DHS' FY 2013 Financial Statements and Internal Control over Financial Reporting	12/11/2013	We recommend that Coast Guard: Establish new or improve existing processes to identify and evaluate lease agreements to ensure that they are appropriately classified as operating or capital, and are properly reported in the financial statements and related disclosures.	C.1.d	USCG		
72	OIG-15-10	Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting	11/14/2014	We recommend that Coast Guard: Adopt policies, procedures, and accounting treatments documented in ad hoc technical accounting research papers into official financial reporting guidance that is distributed agency wide; and refine financial reporting policies and procedures to prescribe process level internal controls at a sufficient level of detail to ensure consistent application to mitigate related financial statement risks.	1.a.b	USCG		
73	OIG-15-10	Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting	11/14/2014	We recommend that Coast Guard: Identify and employ additional skilled resources.	1.a.c	USCG		
74	OIG-15-10	Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting	11/14/2014	We recommend that Coast Guard, establish new or improve existing policies, procedures, and related internal controls to ensure that: Environmental liability schedules are updated, maintained, and reviewed.	1.a.ii	USCG		
75	OIG-15-10	Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting	11/14/2014	We recommend that Coast Guard, establish new or improve existing policies, procedures, and related internal controls to ensure that: Underlying data used in the estimation of environmental liabilities is complete and accurate.	1.a.iii	USCG		
76	OIG-15-10	Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting	11/14/2014	We recommend that Coast Guard, establish new or improve existing policies, procedures, and related internal controls to ensure that: Accrual decisions and/or calculations as well as the validation of prior year accrual amounts are properly reviewed.	1.a.iv	USCG		

	Report No.	Report Title	Date Issued	Recommendation	Rec. No.	DHS Comp.	Questioned Cost (Federal Share)	Funds to be Put to Better Use (Federal Share)
77	OIG-15-10	Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting	11/14/2014	We recommend that Coast Guard: Design and implement controls to appropriately track asset activity at a transaction level and ensure the timely recording of asset additions, deletions, or other adjustments.	1.C.1.a	USCG		
78	OIG-15-10	Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting	11/14/2014	We recommend that Coast Guard: Continue to implement controls over the transfer of completed construction in progress assets to in-use and accurately recording leasehold improvements, asset impairments, and construction in progress activity.	1.C.1.b	USCG		
79	OIG-15-10	Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting	11/14/2014	We recommend that Coast Guard: establish new or improve existing policies, procedures, and related internal controls to sufficiently support personal and real property balances, including electronics, internal-use software, land, buildings and other structures.	1.C.1.d	USCG		
80	OIG-15-10	Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting	11/14/2014	We recommend that Coast Guard: establish new, or improve existing, processes to identify and evaluate lease agreements to ensure they are appropriately classified as operating or capital, and are properly reported in the financial statements and related disclosures.	1.C.1.e	USCG		
81	OIG-15-10	Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting	11/14/2014	We recommend that Coast Guard: Identify and employ additional skilled resources.	1.C.1.f	USCG		
82	OIG-15-55	United States Coast Guard Has Taken Steps to Address Insider Threats, but Challenges Remain	3/27/2015	We recommend that the USCG CIO: Implement software to protect against the unauthorized removal of sensitive information through removable media devices and email accounts.	1	USCG		
83	OIG-15-55	United States Coast Guard Has Taken Steps to Address Insider Threats, but Challenges Remain	3/27/2015	We recommend that the USCG CIO: Implement stronger physical security controls to protect USCG's IT assets from possible loss, theft, destruction, and malicious actions.	2	USCG		
84	OIG-16-06	Independent Auditors' Report on DHS' FY 2015 Financial Statements and Internal Control over Financial Reporting	11/13/2015	We recommend that Coast Guard: Establish new, or improve existing, policies, procedures, and related internal controls.	1.a	USCG		

	Report No.	Report Title	Date Issued	Recommendation	Rec. No.	DHS Comp.	Questioned Cost (Federal Share)	Funds to be Put to Better Use (Federal Share)
85	OIG-16-06	Independent Auditors' Report on DHS' FY 2015 Financial Statements and Internal Control over Financial Reporting	11/13/2015	We recommend that Coast Guard establish new or improve existing policies, procedures, and related internal controls to ensure that: Transactions flowing between various general ledger systems, whether the result of remediation or system limitation manual workarounds, are sufficiently tracked and analyzed to ensure complete and accurate reporting of operational activity and related general ledger account balances.	1.a.ii	USCG		
86	OIG-16-06	Independent Auditors' Report on DHS' FY 2015 Financial Statements and Internal Control over Financial Reporting	11/13/2015	We recommend that Coast Guard: Establish new or improve existing policies, procedures, and related internal controls to ensure: The year-end close-out process, reconciliations, and financial data and account analysis procedures are supported by documentation, including evidence of effective management review and approval; and beginning balances in the following year are determined to be reliable and supported.	1.a.v	USCG		
87	OIG-16-06	Independent Auditors' Report on DHS' FY 2015 Financial Statements and Internal Control over Financial Reporting	11/13/2015	We recommend that Coast Guard establish new or improve existing policies, procedures, and related internal controls to ensure that: All intra-governmental activities and balances are reconciled on a timely basis, accurately reflected in the financial statements, and differences are resolved in a timely manner.	1.a.vi	USCG		
88	OIG-16-06	Independent Auditors' Report on DHS' FY 2015 Financial Statements and Internal Control over Financial Reporting	11/13/2015	We recommend that Coast Guard establish new or improve existing policies, procedures, and related internal controls to ensure that: Adequate understanding and oversight of assumptions used in significant estimates is maintained by Coast Guard management and continued appropriateness of those assumptions are routinely evaluated.	1.a.vii	USCG		
89	OIG-16-06	Independent Auditors' Report on DHS' FY 2015 Financial Statements and Internal Control over Financial Reporting	11/13/2015	We recommend that Coast Guard: Identify and employ additional skilled resources and align them to financial reporting oversight roles.	1.c	USCG		

	Report No.	Report Title	Date Issued	Recommendation	Rec. No.	DHS Comp.	Questioned Cost (Federal Share)	Funds to be Put to Better Use (Federal Share)
90	OIG-16-06	Independent Auditors' Report on DHS' FY 2015 Financial Statements and Internal Control over Financial Reporting	11/13/2015	We recommend that Coast Guard: Develop processes and monitoring mechanisms to track construction-in-progress (CIP) projects at an asset level and continue to implement controls over the transfer of completed CIP assets to in-use and accurately record leasehold improvements, asset impairments, and construction in progress activity.	1.C.1.b	USCG		
91	OIG-16-06	Independent Auditors' Report on DHS' FY 2015 Financial Statements and Internal Control over Financial Reporting	11/13/2015	We recommend that Coast Guard: Design contracts for Coast Guard's major construction projects to isolate costs between development and maintenance (i.e., capitalizable vs. expense), at an individual asset level, in order to enhance traceability of CIP costs.	1.C.1.c	USCG		
92	OIG-16-06	Independent Auditors' Report on DHS' FY 2015 Financial Statements and Internal Control over Financial Reporting	11/13/2015	We recommend that Coast Guard: Establish new or improve existing policies, procedures, and related internal controls to sufficiently review personal and real property activity and balances, including electronics, internal-use software, land, buildings and other structures, and verify costs are appropriate and reflect USCG's business operations during the fiscal year.	1.C.1.e	USCG		
93	OIG-16-06	Independent Auditors' Report on DHS' FY 2015 Financial Statements and Internal Control over Financial Reporting	11/13/2015	We recommend that Coast Guard: Establish new, or improve existing, processes to identify and evaluate lease agreements to ensure they are appropriately classified as operating or capital, and are properly reported in the financial statements and related disclosures.	1.C.1.f	USCG		
94	OIG-16-06	Independent Auditors' Report on DHS' FY 2015 Financial Statements and Internal Control over Financial Reporting	11/13/2015	We recommend that Coast Guard: Develop and implement procedures to support the completeness, accuracy, and existence of all data utilized (e.g., real property multi-use assets) in developing required financial statement disclosures, and related supplementary information, for stewardship property.	1.C.1.h	USCG		
95	OIG-16-06	Independent Auditors' Report on DHS' FY 2015 Financial Statements and Internal Control over Financial Reporting	11/13/2015	We recommend that Coast Guard: Implement accounting and financial reporting processes and an integrated general ledger system that is FFMIA compliant.	1.d	USCG		

	Report No.	Report Title	Date Issued	Recommendation	Rec. No.	DHS Comp.	Questioned Cost (Federal Share)	Funds to be Put to Better Use (Federal Share)
96	OIG-16-06	Independent Auditors' Report on DHS' FY 2015 Financial Statements and Internal Control over Financial Reporting	11/13/2015	We recommend that Coast Guard: Develop a comprehensive understanding of their actuarial evaluations and document the sources of all underlying data and assumptions.	1.e	USCG		
97	OIG-16-15	(U) Fiscal Year 2015 Evaluation of DHS' Compliance with Federal Information Security Modernization Act Requirements for Intelligence Systems	12/14/2015	This recommendation is classified.	2	USCG		
98	OIG-16-15	(U) Fiscal Year 2015 Evaluation of DHS' Compliance with Federal Information Security Modernization Act Requirements for Intelligence Systems	12/14/2015	This recommendation is classified.	3	USCG		
99	OIG-16-15	(U) Fiscal Year 2015 Evaluation of DHS' Compliance with Federal Information Security Modernization Act Requirements for Intelligence Systems	12/14/2015	This recommendation is classified.	4	USCG		
100	OIG-17-12	Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting	11/14/2016	We recommend that DHS develop continuous monitoring and testing of IT general controls to identify weaknesses, assess the resulting risks created by any identified IT deficiencies, and respond to those risks through implementing compensating controls.	2	USCG		
101	OIG-17-12	Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting	11/14/2016	We recommend that Coast Guard establish new, or improve existing, policies, procedures, and related internal controls to ensure that transactions flowing between various general ledger systems, whether the result of balance clean-up activities or system limitation manual workarounds, are sufficiently tracked and analyzed to ensure complete and accurate reporting of operational activity and related general ledger account balances.	5	USCG		

	Report No.	Report Title	Date Issued	Recommendation	Rec. No.	DHS Comp.	Questioned Cost (Federal Share)	Funds to be Put to Better Use (Federal Share)
102	OIG-17-12	Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting	11/14/2016	We recommend that Coast Guard establish new, or improve existing, policies, procedures, and related internal controls to ensure that all non-standard adjustments (i.e., journal entries and top side adjustments) impacting the general ledger are adequately researched, supported, and reviewed prior to their recording in the general ledger.	6	USCG		
103	OIG-17-12	Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting	11/14/2016	We recommend that Coast Guard establish new, or improve existing, policies, procedures, and related internal controls to ensure that the year-end close-out process, reconciliations, and financial data and account analysis procedures are supported by documentation, including evidence of effective management review and approval; and beginning balances in the following year are determined to be reliable and supported.	7	USCG		
104	OIG-17-12	Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting	11/14/2016	We recommend that Coast Guard establish new, or improve existing, policies, procedures, and related internal controls to ensure that all intra-governmental activities and balances are reconciled, accurately reflected in the financial statements, and differences are resolved in a timely manner.	8	USCG		
105	OIG-17-12	Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting	11/14/2016	We recommend that Coast Guard establish new, or improve existing, policies, procedures, and related internal controls to ensure that Management possesses adequate understanding, maintains documentation, exercises oversight of chosen assumptions, and routinely evaluates the completeness and accuracy of underlying data and the continued appropriateness of assumptions used in significant estimates.	9	USCG		
106	OIG-17-12	Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting	11/14/2016	We recommend that Coast Guard establish new, or improve existing, policies, procedures, and related internal controls to increase training and development of existing resources to better align them to financial reporting oversight roles.	10	USCG		

	Report No.	Report Title	Date Issued	Recommendation	Rec. No.	DHS Comp.	Questioned Cost (Federal Share)	Funds to be Put to Better Use (Federal Share)
107	OIG-17-12	Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting	11/14/2016	We recommend that Coast Guard design and implement controls to appropriately track asset activity at the transaction level and ensure the timely recording of asset additions, deletions, or other adjustments.	19	USCG		
108	OIG-17-12	Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting	11/14/2016	We recommend that Coast Guard develop processes and monitoring mechanisms to track CIP projects at an asset level, continue to implement controls over the transfer of completed CIP to in-use assets, and increase monitoring of CIP activity to ensure accurate recording in the general ledger.	20	USCG		
109	OIG-17-12	Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting	11/14/2016	We recommend that Coast Guard involve financial management personnel in the procurement of contracts for Coast Guard's major construction projects to ensure that they are structured to facilitate isolation of costs between development and maintenance (i.e., capitalizable vs. expensed), at an individual asset level, in order to enhance traceability of CIP costs.	21	USCG		
110	OIG-17-12	Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting	11/14/2016	We recommend that Coast Guard adhere to established inventory policies and procedures.	22	USCG		
111	OIG-17-12	Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting	11/14/2016	We recommend that Coast Guard establish new, or improve existing, policies, procedures, and related internal controls to sufficiently review personal and real property activity and balances in order to verify costs are appropriate and reflect USCG's business operations during the fiscal year.	23	USCG		
112	OIG-17-12	Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting	11/14/2016	We recommend that Coast Guard attract and deploy additional skilled resources to support the control environment and provide the necessary financial reporting oversight.	24	USCG		
113	OIG-17-03	AMO and Coast Guard Maritime Missions Are Not Duplicative, But Could Improve with Better Coordination	10/14/2016	We recommend that the Coast Guard Commandant, CBP Commissioner, and U.S. Immigration and Customs Enforcement Director revise the Maritime Operations Coordination Plan to include requirements for coordination and information sharing at all levels, especially the local level.	2	USCG, CBP, ICE		

	Report No.	Report Title	Date Issued	Recommendation	Rec. No.	DHS Comp.	Questioned Cost (Federal Share)	Funds to be Put to Better Use (Federal Share)
114	OIG-16-105	DHS' Use of Reimbursable Work Agreements with GSA	6/23/2016	We recommend that the DHS Under Secretary for Management ensure that deobligation has occurred for the following two reimbursable work agreements that the component was unable to prove had been done. - Coast Guard Reimbursable Work Agreements (RWA) #N3288560 - $43,575 should be deobligated - Coast Guard RWA# B0511609 - $2,779,654 should be deobligated.	3	USCG, MGMT		$2,823,229
115	OIG-16-105	DHS' Use of Reimbursable Work Agreements with GSA	6/23/2016	We recommend that the DHS Under Secretary for Management conduct a review of the following three reconciliation differences for the reimbursable work agreements, determine the reasons for the differences, and make any necessary corrections. - Coast Guard RWA# N3288560 - $12,328,457 expenditure difference - Coast Guard RWA# B0511609 - $320,228 expenditure difference - USCIS RWA# N3322206 - $45,500 expenditure difference.	2	USCIS, USCG, MGMT	$12,694,185	
				Total Monetary Findings			**$12,694,185**	**$2,823,229**
Total Recommendations as of December 31, 2016: 115								