STATEMENT OF JOHN ROTH

INSPECTOR GENERAL

DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTE ON OVERSIGHT AND
MANAGEMENT EFFICIENCY

UNITED STATES HOUSE OF
REPRSENTATIVES

CONCERNING

ASSESSING DHS' PERFORMANCE: WATCHDOG RECOMMENDATIONS TO IMPROVE HOMELAND SECURITY

February 26, 2015

Chairman Perry, Ranking Member Watson Coleman, and Members of the Subcommittee:

Thank you for inviting me here today to discuss our recommendations to improve homeland security. I am pleased to have the opportunity to share our efforts to improve DHS through our independent audits and inspections, as well as our efforts to ensure the integrity of the DHS workforce and its operations.

I would like to focus on some of DHS' challenges, many of which we highlighted in our fiscal year (FY) 2014 report on major management challenges, and some of which at times hamper our efforts to improve the Department's programs and operations. My testimony today will focus on recent and upcoming audits in four areas: unity of effort, acquisition management, IT management, and financial management.

Recent and Upcoming Work

Unity of Effort

Given its history as a group of very diverse agencies and its complex, multifaceted mission, it is not surprising that the Department continues to face challenges transforming itself into a cohesive single agency. To accomplish its mission, DHS must have a strong, yet flexible, central authority that is able to ensure the components collaborate for maximum effectiveness and cost-efficiency. A unified culture within DHS is necessary for better homeland security, as well as deriving efficiencies from the integration of operations. The Secretary's April 2014 Unity of Effort Initiative is a positive step towards achieving that change. In addition, DHS must strengthen its efforts to integrate management operations under an authoritative governing structure capable of effectively overseeing and managing programs that cross component lines.

We have observed that the components often have similar responsibilities and challenges, but many times operate independently and do not unify their efforts, cooperate, or share information. This situation is sometimes exacerbated by components' disregard for DHS' policies. Together, these problems hamper operations and lead to wasteful spending; for instance,

- Last year, we found that DHS did not adequately manage or have the enforcement authority over its components' vehicle fleet operations to ensure right-sizing, that is, to make certain the motor vehicle fleet includes the correct number and type of vehicles. Without a centralized fleet management information system, the Department has to rely on multiple systems that contain inaccurate and incomplete vehicle data. Additionally, each component manages its own vehicle fleet, making it difficult for the DHS Fleet Manager to provide adequate oversight and ensure the components comply with Federal laws, regulations, policies, and directives. We found that the components were operating underused vehicles, which in FY 2012, cost DHS from $35 to $49 million. (*DHS Does Not Adequately Manage or Have Enforcement Authority Over its Component's Vehicle Fleet Operations*, OIG 14-126)

- The Department's failure to adequately plan and manage programs and ensure compliance was also evident in our audit of DHS' preparedness for a pandemic. We found that the

Department did not develop and implement stockpile replenishment plans, sufficient inventory controls to monitor stockpiles, or have adequate contract oversight processes; DHS also did not ensure compliance with its guidelines. Thus, DHS was not effectively managing its stockpile of pandemic equipment and antiviral medications, and components were maintaining inaccurate inventories of pandemic preparedness supplies. Consequently, the Department cannot be certain it has sufficient equipment and medical countermeasures to respond to a pandemic. (*DHS Has Not Effectively Managed Pandemic Personal Protective Equipment and Antiviral Medical Countermeasures*, OIG 14-129)

In FY 2015, we will continue to monitor the Department's efforts toward achieving unity of effort; for example,

- DHS operates a number of training centers to meet the demand for specialized skills across the Department. We have just begun an audit to determine whether DHS' oversight of its training centers ensures the most cost-effective use of resources. Although the Department has made great strides in improving both the quality and availability of training, we believe there may be opportunities to reduce overall cost by identifying redundant capacity.

- Another forthcoming audit focuses on whether DHS has the information it needs to effectively manage its warehouses. Until recently, the components managed their own warehouse needs with little or no joint effort. We expect to publish the final report by June 2015.

Acquisition Management

Acquisition management at DHS is inherently complex and high risk. It is further challenged by the magnitude and diversity of the Department's procurements. DHS acquires more than $25 billion[1] worth of goods and services each year. Although DHS has improved its acquisition processes, many major acquisition programs lack the foundational documents and management controls necessary to manage risks and measure performance. Components do not always follow departmental acquisition guidance, which leads to cost overruns, missed schedules, and mediocre acquisition performance. All of these have an effect on budget, security, and efficient use of resources; for example,

- U.S. Customs and Border Protection (CBP) did not effectively plan and manage employee housing in Ajo, Arizona, and made decisions that resulted in additional costs to the Federal Government, spending about $680,000 for each house that was built, which was significantly more than the Ajo average home price of $86,500. We identified about $4.6 million CBP spent on the project that could have been put to better use. (*CBP Did Not Effectively Plan and Manage Employee Housing in Ajo, Arizona* (Revised), OIG-14-131)

- We recently reported that although CBP's Unmanned Aircraft System program contributes to border security, after 8 years, CBP cannot prove that the program is effective because it has

[1] According to DHS' *FY 2014 Agency Financial Report*, the Department's FY 2014 obligations for "Contractual Services and Supplies" were about $22.6 billion and its obligations for "Acquisition of Assets" were about $3.1 billion.

not developed performance measures. The program has also not achieved the expected results — the aircraft are not meeting flight hour goals, and we found little or no evidence CBP has met its program expectations. CBP anticipated using the unmanned aircraft to patrol more than 23,000 hours per year, but the aircraft logged only a combined total of 5,102 hours, or about 80 percent less than what was anticipated. As a result, CBP has invested significant funds in a program that has not achieved the expected results, and it cannot demonstrate how much the program has improved border security. The $443 million CBP plans to spend on program expansion could be put to better use by investing in alternatives, such as manned aircraft and ground surveillance assets. (*U.S. Customs and Border Protection's Unmanned Aircraft System Program Does Not Achieve Intended Results or Recognize All Costs of Operations*, OIG-15-17)

- In a recent management advisory, we brought to the Department's attention an issue related to CBP's National Aviation Maintenance contract. In 2009, CBP awarded a $938 million contract to Defense Support Services, LLC to maintain about 265 aircraft to fly approximately 100,000 hours per year. Since the contract was awarded, however, the number of CBP aircraft maintained, annual flight hours, and the average age of the aircraft fleet have decreased, while contract costs increased. We were not able to reconcile maintenance labor hours with the hours the contractor charged CBP because of inconsistent and unreliable data. (*U.S. Customs and Border Protection's Management of National Aviation Maintenance Activities*, Management Advisory)

Given the magnitude and risks of the Department's acquisitions, we will continue to invest resources in this critical area; for instance,

- In FY 2015, we plan to audit CBP's acquisition of an integrated fixed tower (IFT) system. IFT systems are intended to assist agents in detecting, tracking, identifying, and classifying items of interest along our borders through a series of fixed sensor towers. In February 2014, CBP awarded $145 million to begin work on the IFT acquisition program, a spin-off of CBP's $1 billion SBInet acquisition. The acquisition is currently in schedule breach. An audit at this point in the program's life cycle will be useful in identifying program challenges and may help prevent further schedule breaches.

- We are also planning an audit to determine whether the USCG is effectively managing the acquisition of eight Legend-class National Security Cutters, which will replace its 1960s-era High Endurance Cutters. In 2012, GAO reported that the cost of the USCG's plan to acquire the final two cutters is not covered by the USCG's current 5-year budget plan. Thus, there may be a significant mismatch between expected capital investment funding and the estimated life cycle costs for the project.

As these examples illustrate, we are moving towards a more proactive approach by performing audits throughout the acquisition process. This approach would allow for course corrections early in the acquisition lifecycle before full investment in a program occurs — addressing cost, schedule, and performance problems as they occur, thus protecting a long-term investment.

Cybersecurity and IT Management

DHS continues to face challenges in protecting its IT infrastructure, as well as ensuring that its infrastructure supports its mission needs and operates efficiently. Recent audits highlight some of these challenges:

- As we reported in December 2014, the Department made progress in improving its information security program. Although it has transitioned to a risk-based approach for managing IT security, the components' lack of compliance with existing security policies and weaknesses in DHS' oversight and enforcement of these policies undermines the Department's efforts. Additionally, DHS and its components continued to operate information systems without the proper authority, hindering protection of sensitive information. There are some indications that DHS may not be properly inventorying its systems or that components may be procuring or developing new systems independently. Components also did not mitigate security vulnerabilities in a timely manner. (*Evaluation of DHS' Information Security Program for Fiscal Year 2014*, OIG-15-16)

- In July 2014, the National Protection and Programs Directorate (NPPD) made progress expanding its Enhanced Cybersecurity program to share cyber threat information with qualified Commercial Service Providers and ultimately to 16 critical infrastructure sectors. But NPPD's limited outreach and resources slowed the expansion. NPPD also relied on manual reviews and analyses to share cyber threat information, which led to inconsistent quality in cyber threat indicators. (*Implementation Status of Enhanced Cybersecurity Services Program*, OIG-14-119)

- We reported on problems with the Electronic Immigration System (ELIS), which U.S. Citizenship and Immigration Services (USCIS) uses in its adjudication process. The system's 29 commercial software products make it difficult to make changes in the system. Although ELIS was designed to improve efficiency, time studies showed that adjudicating using paper-based processes was faster than using the complex computer system. USCIS staff also said it takes longer to process adjudications using the Enterprise Document Management System (EDMS), which they use to view and search electronic copies of paper-based immigration case files. Although digitizing files reduces document delivery time, staff said using EDMS is burdensome. (*U.S. Citizenship and Immigration Services Information Technology Management Progress and Challenges*, OIG-14-112)

- In March 2014, we reported on EINSTEIN 3 Accelerated (E^3A), an automated process for collecting network security information from participating Federal agencies. NPPD has begun deploying E^3A and expects to reach full operating capability by the end of FY 2015. However, we concluded that NPPD needs to strengthen its monitoring of E^3A's implementation and improve its ability to handle personally identifiable information as the program matures. (*Implementation Status of EINSTEIN 3 Accelerated*, OIG-14-52)

Financial Management

Financial statement audits

Congress and the public must be confident that DHS is properly managing its finances to make informed decisions, manage government programs, and implement its policies. In FY 2014, DHS obtained an unmodified (clean) opinion on all financial statements for the first time in its history. This was a significant achievement that built on previous years' successes; yet, it required considerable manual effort to overcome deficiencies in internal control and a lack of financial IT systems functionality.

Many key DHS financial systems do not comply with Federal financial management system requirements. Limitations in financial systems functionality add substantially to the Department's challenge in addressing systemic internal control weaknesses and limit its ability to leverage IT systems to process and report financial data efficiently and effectively. In FY 2015 and beyond, DHS will need to sustain its progress in achieving an unmodified opinion on its financial statements and work toward building a solid financial management internal control structure.

Grant Management (FEMA)

FEMA continues to experience challenges managing the immense and risky disaster assistance program. Currently, every state and most of the U.S. possessions have open disasters that include more than 100,000 grant applicants spending more than $50 billion on more than 600,000 disaster assistance projects. Last year, we issued *Capping Report: FY 2013 FEMA Public Assistance and Hazard Mitigation Grant and Subgrant Audits* (OIG-14-102-D), which summarized the results of our disaster assistance audits for the last 5 years. Of the $5.9 billion we audited, disaster assistance recipients did not properly spend $1.36 billion, or an average of 23 percent, of the disaster assistance grants.

The Department also provides Homeland Security Grant Program (HSGP) funds to state, territory, local, and tribal governments to enhance their ability to respond to terrorist attacks and other disasters. Since 2005, we have conducted 74 separate audits covering more than $7 billion in HSGP funds awarded to all 50 States, 6 urban areas, 5 U.S. territories, and the District of Columbia. Although we determined that in most instances the states complied with applicable laws and regulations, we issued more than 600 recommendations for improvement to FEMA, almost 90 percent of which have been resolved. Most of the recommendations were related to strategic homeland security planning, timely obligation of grant funds, financial management and reporting, and sub-grantee compliance monitoring.

We will continue to look for ways to help FEMA improve grant management in FY 2015. For instance, we are currently undertaking a capstone review to measure the impact of FEMA's corrective actions as they specifically address these recurring challenges. We anticipate that our assessment will further strengthen the level of national preparedness by helping to better inform the agency's future administration and investment of taxpayer dollars.

We are also conducting an audit of approximately $2 billion awarded through FEMA's Assistance to Firefighters Grant and Staffing for Adequate Fire and Emergency Response Grants programs. These grants are awarded directly to fire departments (volunteer, combination, and career), unaffiliated Emergency Medical Service (EMS) organizations, or volunteer firefighter interest organizations. The audit will determine if FEMA ensures that these grant funds are expended appropriately.

Challenges

Meeting the Risk

We must focus our limited resources on issues that make a difference, especially those that may have a significant impact on the Department's ability to fulfill its strategic missions. At the beginning of each year, we initiate a risk-based planning process by identifying high impact programs and operations that are critical to the Department's mission or integrity. Once we identify the high impact areas, we evaluate all the projects that have been proposed throughout the previous year.

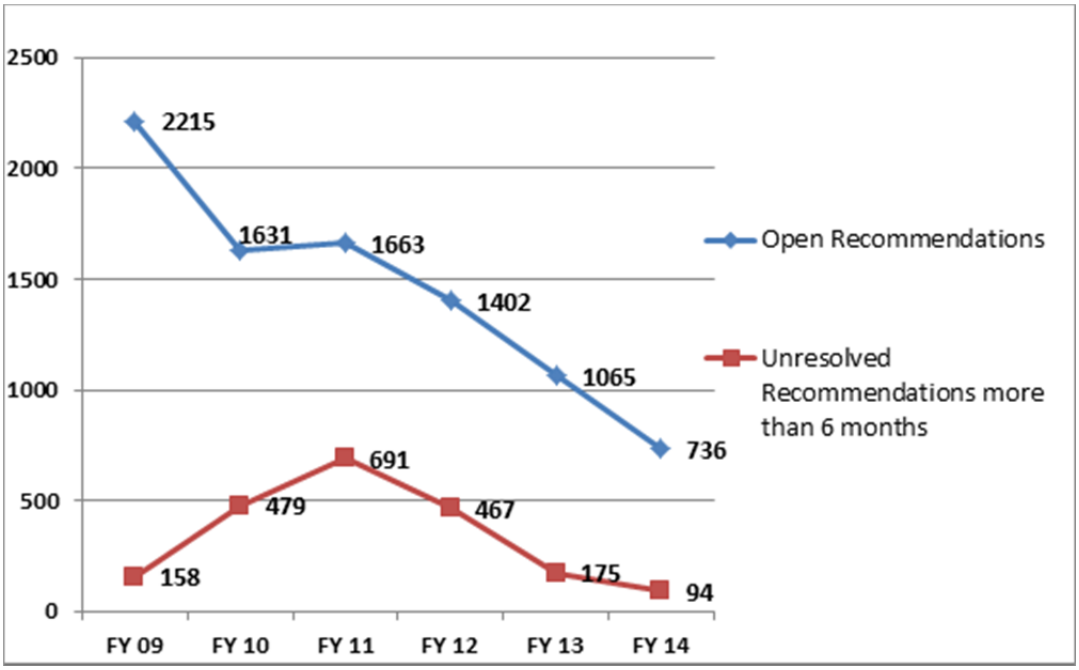
As we planned our work for FY 2015, we began with two priorities: to aid the Department in achieving its critical missions and priorities and to ensure the proper stewardship and integrity of Department programs and resources. We also conduct legislatively mandated work and make an earnest effort to address the concerns of Congress and the Department, along with our other stakeholders. In FY 2015, our work will focus on determining the effectiveness of the Department's efforts to (1) prevent terrorism and enhance security; (2) enforce and administer our immigration laws; (3) secure and manage our borders; (4) strengthen national preparedness and resilience to disasters; and (5) safeguard and secure the Nation's cyberspace. We will also continue our efforts to promote management stewardship and ensure program integrity.

Our Annual Performance Plan and our current list of Ongoing Projects are published on our website to better inform the Congress and the public regarding our work.

Audit Follow-up

Audit follow-up is an integral part of good management; it is a shared responsibility of both auditors and agency management officials. The Department has made great strides in closing recommendations. For example, as shown in the following chart and attachment 1, DHS reduced the number of unresolved, open recommendations more than 6 months old from a high of 691 in FY 2011 to 94 in FY 2014. In parallel, the number of recommendations categorized as "resolved-open" (recommendations that the Department agreed to but has not yet implemented) steadily declined from a high of 1663 in FY 2011 to 736 in FY 2014. DHS' goal is to have zero financial statement-related recommendations categorized as "open-unresolved" by March 30, 2015. This progress largely results from increased focus by the Department through the audit liaisons and increased communication with our office; we sincerely appreciate the personnel and resources the Department has dedicated to this effort. In addition, we recently began publishing a quarterly report of open recommendations over six months old on our public website in an effort to make this process more transparent to Congress and the public.

Recommendation Trends FY 2009 - 2014



We need to do more to ensure that Department and component management fully implements corrective actions. To that end, we are initiating "verification reviews." These limited-scope reviews will focus on our most crucial recommendations, examining whether the recommendations were implemented and whether the actions taken had the intended effect; for example,

- One of our verification reviews will determine if USCG implemented recommendations from our 2012 audit on the USCG's Sentinel Class Fast Response Cutter (FRC). In September 2008, the USCG awarded an $88.2 million fixed-price contract for the detailed design and construction of the lead FRC. The estimated $1.5 billion contract contains 6 options to build a maximum of 34 cutters. We found that USCG's schedule-driven strategy allowed construction of the FRCs to start before operational, design, and technical risks were resolved. Consequently, six FRCs under construction needed modification, which increased the total cost of the acquisition by $6.9 million and caused schedule delays of at least 270 days for each cutter. This aggressive acquisition strategy also allowed the USCG to procure 12 FRCs before testing in actual operations. We made four recommendations designed to eliminate this risk in future acquisitions and one recommendation to address the current FRC acquisition. (*U.S. Coast Guard's Acquisition of the Sentinel Class – Fast Response Cutter*, OIG-12-68)

- We will also follow up on the recommendations from our report on DHS' oversight of interoperable communications. During the audit, we tested DHS radios to determine whether DHS components could talk to each other in the event of an emergency. They could not. Only 1 of 479 radio users we tested — or less than 1 percent — could access and use the specified common channel to communicate. Further, of the 382 radios tested, only 20 percent (78) contained all the correct program settings for the common channel. In our verification

review, we will determine whether the Department created a structure with the necessary authority to ensure that the components achieve interoperability, as well as policies and procedures to standardize Department-wide radio activities. (*DHS' Oversight of Interoperable Communications*, OIG-13-06)

We believe verification reviews such as these will result in increased commitment by the components to enact change.

Transparency of Reports

The *Inspector General Act* contemplates that my reports, to the greatest possible extent, be available to the public. Openness and transparency are critical to good government, and the Act allows me to publish my reports except in three narrow circumstances: first, where disclosure of the information is specifically prohibited by law; second, where specifically prohibited from disclosure by executive order in the interest of national defense, national security, or in the conduct of foreign affairs; and third, where part of an ongoing criminal investigation.

The Department often raises objections to the publication of certain information in our reports, often marking parts of our reports as "For Official Use Only" or "Law Enforcement Sensitive." These designations are not recognized in the law, and in my experience they risk being used to attempt to avoid revealing information that is embarrassing to the agency involved. However, sometimes such information, if disclosed, could cause harm to DHS programs and operations.

In those situations, I use my discretion to redact information in our public report. However, in order to properly exercise my discretion in an informed and responsible manner, I require such requests to come from the component or agency head, coupled with an articulation of the *actual, specific* harm that would result from disclosure. Too often, the fear of harm is highly speculative, and fails to balance the need for transparency against the risks of disclosure.

Recently, we have had issues with the Transportation Security Administration (TSA) designating certain material as "Sensitive Security Information" (SSI) within an audit report concerning the information technology operations at John F. Kennedy airport in New York. The designation of SSI is in the absolute and unreviewable discretion of the Administrator of TSA and improper disclosure of it carries with it civil and administrative penalties. What was especially troubling about this episode, in my view, was the length of time it took — nearly 6 months — to get a resolution of the issue, the fact that my security experts who wrote the report were confident that the general and non-specific manner in which they wrote the report would not compromise TSA's computer security, and that the similar information had been published in previous audit reports without objection.

The SSI designation is a useful tool to protect sensitive transportation security information in a manner that gives some flexibility to TSA. However, I am worried that SSI can be misused, as I believe it has been here, to prevent embarrassment. We intend to conduct a formal review of TSA's administration of the SSI program, and report those results to the Secretary and the congressional committees with oversight over the program.

Resources

The budget for our office is relatively tiny — we represent just 0.23 percent of the DHS budget, yet we have an outsize impact on the operation of the Department.

For every dollar given to the OIG, we return more than $7 in savings, as reflected by the statutory performance measures set forth in the *Inspector General Act*. This vastly understates our performance, because much of our best work — audit and inspections reports that shed light on problematic aspects of programs, for example — don't carry with it a cost savings, but the value to the American taxpayer is incalculable.

Notwithstanding the demonstrated contributions of our office, our budget has actually shrunk by about 1 percent since FY 2012. As a result, our on-board strength from FY 2012 to this year has decreased by about 15 percent. We have been forced to cut training to less than a third of what we have determined to be appropriate, reducing our ability to do our job and decreasing morale. This includes training for our auditors necessary under the *Inspector General Act*, as well as training for our Special Agents to keep them safe.

Yet, during this same time, DHS' authorized workforce grew by about 5,000, representing a 2.3 percent increase. The Department continues to grow, but the Inspector General's office — the one entity within the Department designed to save money and create efficiency — shrinks.

This, I believe, represents a false economy.

Working with Congress

We are proud of our work and the success we have had pointing out challenges the Department needs to overcome and recommending ways to resolve issues and improve programs and operations. However, it is your legislative efforts that enhance the significance of our work and create an even greater impact on the Department. By introducing and passing legislation, you show that you trust in us and have faith in our work. This validation spurs those who need to act to ensure we protect this Nation and use taxpayer dollars effectively; for example,

- S. 159, which was referred to the Senate Committee on Homeland Security and Government Affairs on January 13, 2015, resulted from our recent report on CBP's Unmanned Aircraft System (UAS) Program. The bill requires DHS to use its UAS for surveillance of the entire Southern border and report performance indicators such as flight hours, detections, apprehensions, and seizures. It also prevents DHS from procuring additional UAS until it operates its current fleet for at least 23,000 hours annually. (*U.S. Customs and Border Protection's Unmanned Aircraft System Program Does Not Achieve Intended Results or Recognize All Costs of Operations*, OIG-15-17)

- H.R. 719, the TSA Office of Inspection Accountability Act of 2015, which passed the House on February 10, 2015, resulted from our report on TSA's Office of Inspection. It requires TSA to reclassify criminal investigators if less than 50 percent of their time is spent performing criminal investigative duties. The bill also requires the Assistant Secretary to estimate the cost savings to the Federal government resulting from such reclassification. (*Transportation Security Administration Office of Inspection's Efforts To Enhance Transportation Security*, OIG-13-123)

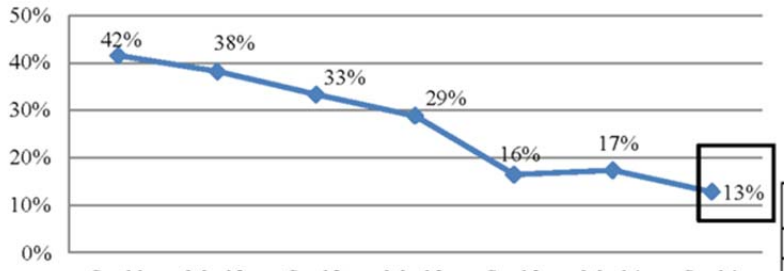
- H.R. 615, which passed the House on February 2, 2015, resulted from our report on DHS's Oversight of Interoperable Communications. This bill would amend the *Homeland Security Act of 2002* to require the Department to take administrative action to achieve and maintain interoperable communications capabilities among its components. (*DHS' Oversight of Interoperable Communications*, OIG-13-06)

We appreciate your efforts and hope that we can continue to count on you in the future. For our part, we intend to continue accomplishing our mission to the best of our ability.

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

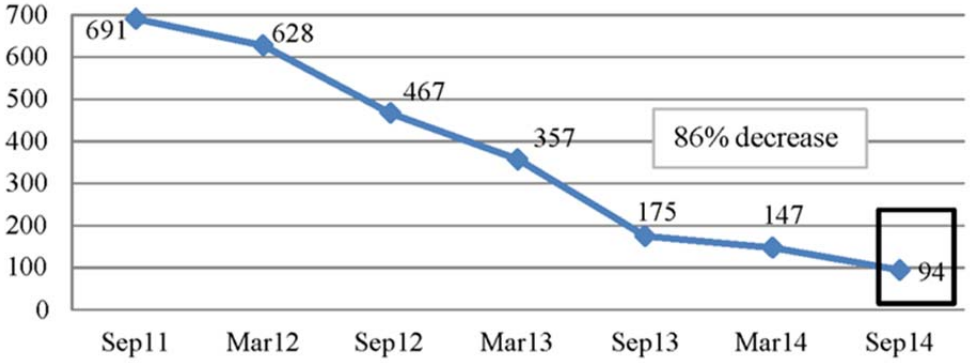
Attachment 1
Status of OIG Recommendations

Percentage of Total Open OIG Recommendations
Unresolved More than 6 Months*



Goals per OCFO Strategic Plan	
FY 15	10%
FY 16	5%
FY 17	3%

Total Open OIG Recommendations
Unresolved More than 6 Months*



*Includes performance, financial statement, and grant-related disaster assistance

Attachment 2
OIG Reports Referenced in This Testimony

DHS Does Not Adequately Manage or Have Enforcement Authority Over its Component's Vehicle Fleet Operations, OIG 14-126, August 2014

DHS Has Not Effectively Managed Pandemic Personal Protective Equipment and Antiviral Medical Countermeasures, OIG 14-129, August 2014

CBP Did Not Effectively Plan and Manage Employee Housing in Ajo, Arizona (Revised), OIG-14-131, September 2014

U.S. Customs and Border Protection's Unmanned Aircraft System Program Does Not Achieve Intended Results or Recognize All Costs of Operations, OIG-15-17, December 2014

U.S. Customs and Border Protection's Management of National Aviation Maintenance Activities, CBP Management Advisory, January 2015

Evaluation of DHS' Information Security Program for Fiscal Year 2014, OIG-15-16, December 2014

Implementation Status of Enhanced Cybersecurity Services Program, OIG-14-119, July 2014

U.S. Citizenship and Immigration Services Information Technology Management Progress and Challenges, OIG-14-112, July 2014

Implementation Status of EINSTEIN 3 Accelerated, OIG-14-52, March 2014

Capping Report: FY 2013 FEMA Public Assistance and Hazard Mitigation Grant and Subgrant Audits, OIG-14-102-D, June 2014

U.S. Coast Guard's Acquisition of the Sentinel Class – Fast Response Cutter, OIG-12-68, August 2012

DHS' Oversight of Interoperable Communications, OIG-13-06, November 2012

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