Major Management and Performance Challenges Facing the Department of Homeland Security

Homeland Security

DHS OIG HIGHLIGHTS
Major Management and Performance
Challenges Facing the Department of Homeland Security

Why We Did This Report

The *Reports Consolidation Act of 2000* (Public Law 106-531) requires the Office of Inspector General to update our assessment of the Department of Homeland Security's (DHS) major management and performance challenges annually.

What We Recommend

This report does not contain any recommendations.

What We Found

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.

This report identifies major challenges that affect the Department as a whole, as well as its individual components, who work together to achieve this multi-faceted mission. The following list represents the nine areas of most persistent concern for the Department:

- DHS Management and Operations Integration
- Acquisition Management
- Financial Management
- Information Management and Technology
- Transportation Security
- Border Security and Immigration Enforcement
- Disaster Preparedness and Response
- Infrastructure Protection and Cybersecurity
- Employee Accountability and Integrity

Within each of the nine areas are specific challenges the Department faces in supporting an engaged, connected workforce; identifying and monitoring business processes that are understandable and streamlined; and designing and implementing innovative technologies that address mission needs. Without the right processes and technology, the Department's strongest asset — its people — may be hampered in their ability to accomplish the Department's mission most effectively and efficiently.

November 13, 2015

MEMORANDUM FOR: The Honorable Jeh Johnson
Secretary

FROM: John Roth
Inspector General

SUBJECT: *Major Management and Performance Challenges Facing the Department of Homeland Security*

Attached for your information is our annual report, *Major Management and Performance Challenges Facing the Department of Homeland Security*. A summary of the report will be included in the Department of Homeland Security 2015 *Annual Financial Report*.

Please call me with any questions, or your staff may contact Mark Bell, Assistant Inspector General for Audits, at (202) 254-4100.

Attachment

Major Management and Performance Challenges Facing the Department of Homeland Security

The attached report presents our fiscal year (FY) 2015 assessment of DHS' major management and performance challenges. As required by the *Reports Consolidation Act of 2000,* we update our assessment of management challenges annually.[1] In this report, the Office of Inspector General (OIG) summarizes what we consider the most serious management and performance challenges to both the Department as a whole, as well as individual components. We also assess the Department's progress in addressing those challenges.

DHS' vision is to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards, where American interests, aspirations, and way of life can thrive. With a budget of about $61 billion spread across a multitude of programs and operations, it is imperative that DHS continue to work as one. To attain these goals, the *2014 Quadrennial Homeland Security Review* identified five homeland security missions:

1. Prevent terrorism and enhance security
2. Secure and manage our borders
3. Enforce and administer our immigration laws
4. Safeguard and secure cyberspace
5. Strengthen national preparedness and resilience

This year, we have identified nine areas representing major challenges the Department must address and ultimately overcome if it is to better accomplish its mission. Within each area, we have observed challenges in coordinating people, processes, and technology. Specifically, the Department faces challenges in ensuring strong management practices and effective oversight; implementing and enforcing consistent, clear guidance; tracking and collecting data that can be used to make effective decisions; and deploying technology that meets mission needs. The following list represents the nine areas of most persistent concern for the Department:

- DHS Management and Operations Integration
- Acquisition Management
- Financial Management
- Information Management and Technology
- Transportation Security

---

[1] Public Law 106-531, November 22, 2000.

- Border Security and Immigration Enforcement
- Disaster Preparedness and Response
- Infrastructure Protection and Cybersecurity
- Employee Accountability and Integrity

Without adequate oversight and understandable guidance, streamlined processes and reliable data, and the right technology, the Department risks duplication of effort, poor stewardship of taxpayer dollars, and investments that are not cost-effective. Furthermore, without these elements, the Department's strongest asset — its people — may not be able to help DHS accomplish its vital mission most effectively and efficiently.

DHS Management and Operations Integration

Strong management of Department programs requires accurate and reliable data; clear and well communicated guidance; and a collaborative, unified environment. In FY 2015, we identified cross-cutting programs in which better management, oversight, and guidance could have improved transparency, effectiveness, and efficiency.

The Department does not always implement processes to collect, verify, and track data necessary to make informed decisions or ensure the most cost efficient use of resources. Specifically, we reported that DHS cannot effectively manage its warehouse needs because some components do not accurately track inventories of their warehouses. We found buildings that should not have been on the Department's warehouse inventory, as well as buildings that should have been classified as warehouses but were not. Department management also did not know enough about what DHS components store in their warehouses. Without reliable information, DHS management cannot make informed decisions to consolidate or close warehouses, demonstrate compliance with space reduction requirements, or reduce unnecessary costs.

We determined through an audit of DHS' travel reservation system that the Department was not requiring components to track employees' justifications for using offline travel reservations. Offline reservations, which are made by phone, cost $23 to $27 more per transaction than making an online reservation. Because components were not tracking these justifications, it was difficult to determine whether offline travel fees were excessive. As a result of our audit, the Department began taking steps to use the online travel reservation system more effectively.

In our annual charge card risk assessment, we found that the Department did not adequately oversee purchase and travel card programs. As a result, there is a moderate risk that the Department's internal controls will not prevent illegal, improper, or erroneous purchases. The Department has begun taking steps to address challenges and is in the process of updating its charge card manuals and oversight plans.

Two years after we released a report on DHS' lack of interoperable radio communications, we discovered that components still cannot communicate effectively on a single radio channel during emergencies, daily operations, and planned events. The Department has developed a draft communications interoperability plan and guidance to standardize radio activities, but could not provide a timetable for finalizing and disseminating this guidance. Also, the National Protection and Programs Directorate (NPPD) and the Federal Emergency Management Agency (FEMA) could coordinate better to issue clear, consistent guidance, which would help prevent DHS grantees from purchasing non-interoperable communications equipment. As a result of our audits, DHS has taken measures to improve communications interoperability, including replacing legacy and obsolete equipment and training DHS users on interoperability and radio capabilities.

Moving Forward

The Department has made great strides in closing recommendations. DHS reduced the number of unresolved, open recommendations more than 6 months old from a high of 691 in FY 2011 to 21 in FY 2015. In parallel, the number of open recommendations — categorized as both unresolved and resolved — steadily declined from a high of 1,663 in FY 2011 to 583 in FY 2015. This progress largely results from increased focus and effort by the Department through its audit liaisons and increased communication with our office.

Addressing the Department's oversight, management, and coordination challenges requires a commitment to building — and sustaining — a culture that recognizes the need to act in a more unified, inclusive, and transparent way. The Secretary's Unity of Effort initiative is a positive step toward achieving this cultural change, and the Department has taken steps to implement this initiative. The Department established a Unity of Effort Integration Office to synchronize the major Departmental planning, programming, budgeting, and joint operations decision processes. This office serves as the Executive Agent for two leadership forums — the Senior Leader's Council and the Deputy's Management

Action Group. These groups provide guidance and recommendations to the Department's leadership to foster informed discussion on cross-component and key departmental issues. The Department established joint task forces, a joint requirements council, and acquisition reforms. It also is developing a number of human capital initiatives, including a new Department-wide approach to joint rotational duty assignments.

DHS must use these forums and other initiatives to continue to ensure the components collaborate for maximum effectiveness and cost efficiency. In addition, DHS must continue to strengthen its efforts to provide effective oversight and management of department-wide programs and programs that cross component lines.

Acquisition Management

Acquisition management — a function critical to the fulfillment of all DHS missions — is inherently complex and high risk. It is further challenged by the magnitude and diversity of the Department's procurements. DHS' yearly spending on contractual services and supplies, along with acquisition of assets, exceeds $25 billion.[2] The Department has improved its acquisition processes and taken steps to improve oversight of major acquisition programs, but challenges to cost-effectiveness and efficiency remain.

Our FY 2015 acquisition audits illustrate ongoing challenges, as well as progress. For instance, the Department encourages components to develop their own policies and guidance for non-major programs — acquisitions with life cycle costs of less than $300 million — as long as they are consistent with the spirit and intent of department-wide guidance. We found that the Science and Technology Directorate (S&T) did not have guidance for its non-major acquisitions, which contributed to the termination of a contract after an investment of more than $23 million for a prototype that was close to delivery. As a result, S&T may have wasted up to $23 million in incurred and potential contract termination costs. In addition, S&T's lack of policies and procedures may hinder its ability to make well-informed decisions about all of its contracts, valued at $338 million in FY 2013.

---

[2] 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.

In contrast, the U.S. Secret Service's acquisition management office exemplifies what can be accomplished when components follow the Department's acquisition guidance — adequate oversight and management of acquisitions with only minor issues that were promptly corrected. In February 2015, we reported that the Secret Service's acquisition management program office had adequate oversight and management of its acquisition process, complied with DHS acquisition guidance, and had implemented some best practices. The Secret Service fully implemented our recommendations to further strengthen acquisition management by finalizing guidance for its acquisitions with life cycle costs of less than $300 million (the majority of its investments) and selecting a Component Acquisition Executive.

U.S. Customs and Border Protection's (CBP) Unmanned Aircraft System (UAS) is an example of components' ongoing tendency to acquire systems before adequately defining requirements or developing performance measures. This can result in expensive assets that are underused and may not be adding sufficient value to border security. From FYs 2005 to 2013, CBP invested about $360 million in UAS, which includes Predator B unmanned aircraft, related equipment, such as ground control stations, as well as personnel, maintenance, and support. After 8 years and significant investment, however, CBP could not demonstrate how much UAS has improved border security, largely because the program lacks performance measures. The program also failed to achieve expected results, including aircraft flying only about 20 percent of anticipated flight hours. Furthermore, CBP did not accumulate and report UAS' true cost. We estimate that it cost at least $62.5 million to operate UAS in FY 2013, or about $12,255 per flight hour. As a result of our audit, CBP agreed to establish program goals and performance measures. The Department agreed to conduct an independent study before acquiring more unmanned aircraft and establish a DHS-wide policy for accumulating all program costs. The Department also established a charter for the Flight Hour Program Working Group, which is committed to transparent cost accounting for all DHS aviation programs.

Once acquired, to protect the Department's investments, components must properly manage assets throughout their life cycle. Our reviews of equipment maintenance contracts revealed that components need to improve their oversight to ensure contractors provide required services and to make certain maintenance deficiencies, which could endanger the public, are corrected. Specifically, in May 2015, we reported that the safety of airline passengers could be compromised by the Transportation Security Administration's (TSA) inadequate oversight of four contracts — valued at about $1.2 billion — that cover 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, is ready for operational use, and is operating at its full capacity. In response to our recommendations, TSA agreed to develop, implement, and enforce policies and procedures to ensure its screening equipment is maintained as required and is fully operational while in service.

Similarly, our audit of CBP's non-intrusive inspection equipment maintenance contracts — valued at approximately $90.4 million — showed that CBP did not ensure contractors properly maintained cargo and conveyance screening equipment at ports of entry. As a result, CBP's non-intrusive inspection equipment may not retain its full functionality or reach its maximum useful life. CBP agreed with our recommendation to implement a plan to monitor service contractors' performance, including validation steps for contractor-submitted maintenance data.

We also issued a management advisory on CBP's national aviation maintenance activities. In 2009, CBP awarded a $938 million contract to maintain about 265 aircraft to fly approximately 100,000 hours per year. Since CBP awarded the contract, however, the number of aircraft maintained, annual flight hours, and the average age of the aircraft fleet decreased, while contract costs increased. Additionally, the safety and cost of operating aircraft may be affected by CBP's lack of guidance for addressing and reporting maintenance deficiencies. CBP's Office of Air and Marine plans to better disseminate corrective action reports for maintenance deficiencies and make them accessible to all maintenance officers.

Moving Forward

The Department has made significant progress in awarding contracts through a full and open competitive process. In its first 6 years, from FYs 2003 through 2008, DHS' spending on noncompetitive contracts grew from $655 million to $3.5 billion. Then, largely due to the Department's response to recommendations from OIG and the Government Accountability Office (GAO), spending on noncompetitive contracts fell from $3.5 billion in 2008 to below $400 million in FYs 2012 through 2014.

The urgency and complexity of DHS' mission will continue to demand rapid pursuit of major investment programs. As DHS continues to build its acquisition management capabilities, OIG will keep investing

resources to evaluate this critical area. Increased commitment by the components will effect real and lasting change. This commitment includes adhering to departmental acquisition guidance, adequately defining requirements, developing performance measures before making new investments, and dedicating sufficient resources to contract oversight. All of this will better support DHS' missions and save taxpayer dollars.

Financial Management

The Federal Government must be an effective steward of taxpayer dollars. Sound financial practices and related management operations, reliable financial systems, and effective internal controls are essential to providing reliable, timely financial information to support management decision making necessary to achieve DHS' mission. 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. An effective internal control structure is integral to management and provides a framework for effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations.

DHS obtained an unmodified (clean) opinion on all financial statements in FY 2015. In achieving this opinion, the Department continued to build on last year's success; however, similar to prior years, it required considerable manual effort to overcome deficiencies in internal control and a lack of financial system functionality.

In FY 2014, the independent auditors identified four material weaknesses, three of which persisted into FY 2015 — weaknesses in financial reporting; information technology (IT) controls and financial system functionality; and property, plant, and equipment (PP&E). The Department received an adverse opinion on internal control over financial reporting because of the existence of these material weaknesses. DHS needs to continue its remediation efforts to eliminate the remaining weaknesses and obtain an unqualified (clean) opinion on internal control over financial reporting.

Financial reporting continues to be a challenge for the Department. Although the Department continues to implement corrective action plans and made progress in some areas, deficiencies remain. Several components including the United States Coast Guard (Coast Guard),

Immigration and Customs Enforcement (ICE), Management Directorate (MGMT), NPPD, and S&T contributed to a material weakness in financial reporting in FY 2015. The Coast Guard's financial reporting organizational structure lacks a sufficient number of skilled resources with adequate overall entity and financial acumen to provide appropriate financial reporting oversight necessary to monitor the Coast Guard's decentralized financial operations. Although MGMT, NPPD, and S&T have assumed more responsibilities for their financial management functions, and not simply rely on ICE as the service provider,[3] they did not fully design and/or implement internal controls over financial reporting.

During FY 2015, DHS components made some progress in remediating findings regarding IT controls and financial system functionality reported in FY 2014. As a result, the auditors closed about 24 percent of prior year IT findings. However, they identified 38 new findings at several DHS components in FY 2015. CBP, FEMA, and the Coast Guard had the greatest number of new findings. Many key DHS financial systems do not comply with Federal financial management system requirements, as defined in the *Federal Financial Management Improvement Act of 1996*. The Department lacks sufficient manual mitigating controls to overcome these deficiencies. 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.

A material weakness in PP&E continued to exist in FY 2015. DHS' PP&E includes aircraft, vessels, vehicles, land, structures, facilities, software, and other equipment. The Coast Guard maintains about 50 percent of DHS's PP&E. During FY 2015, the Coast Guard completed its remaining remediation activities involving enrolling assets into the property system. This was the culmination of a long-term effort and represents a significant accomplishment. However, the Coast Guard continued "clean-up" activities and did not complete design and implementation of sufficient internal controls. Additionally, the Coast Guard continued to identify errors in property balances throughout the year. Internal control deficiencies noted in NPPD's financial reporting also contributed to weaknesses in PP&E and led to NPPD contributing to DHS's material weakness over PP&E.

---

[3] MGMT, NPPD, and S&T used ICE as a general ledger service provider, and for several years relied on ICE to ensure financial statements integrity.

DHS also remediated many of the conditions that contributed to a material weakness in budgetary accounting in prior years. This resulted in the auditors downgrading the material weakness to a significant deficiency in FY 2015.

Moving Forward

The Department and its senior management continued their commitment to identifying areas for improvement, developing and monitoring corrective actions, and establishing and maintaining effective internal controls over financial reporting this past fiscal year. Looking forward, 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 in FY 2016 and beyond.

According to the Department, it continues to make progress with its decentralized approach to modernizing financial systems across the Department. The Department's first component financial services modernization initiative was completed at the Federal Law Enforcement Training Center in December 2014. The Domestic Nuclear Detection Office (DNDO) migrated to its new Federal Shared Services Provider's (FSSP) financial services system in November 2015. DNDO was the first DHS component to migrate to a FSSP, while TSA and the Coast Guard are currently in the implementation phase. DHS also reports that through this initiative it will be able to manage its resources better, provide enterprise-level information more quickly to support critical decision making, and further the Department's efforts to standardize business processes and data structures where possible.

Information Management and Technology

IT investments play a critical role in enabling the Department to accomplish its diverse, complex, and evolving missions. New technologies emerge at a rapid pace, security threats grow increasingly sophisticated, and there are fewer resources and dollars government-wide. This requires components to leverage the best available IT and information management practices to support the Department's mission. In FY 2015, we found that DHS continued to face challenges in implementing key IT management processes.

Planning and investing in IT systems that aid DHS personnel in achieving mission operations is critical. FEMA spent about $284 million

over 10 years on its Logistics Supply Chain Management System, but could not be certain the system would be effective during a catastrophic disaster. Specifically, it could not interface with the logistics management systems of FEMA's partners, nor did it allow FEMA real-time visibility over all supplies shipped by its partners. In addition, when the system became fully operational, 19 months after originally scheduled, it could not perform as originally planned. As a result of our audit, FEMA took action to close 6 of the 11 recommendations to improve the effectiveness of its supply chain management system, but still could not ensure the system meets necessary mission capabilities.

We also identified a number of challenges to the Coast Guard's planning and implementation of mission-critical systems. Specifically, the Coast Guard had not addressed how it would meet the critical technology needs of its aircraft and legacy ships. Due to significant budget reductions, the Coast Guard did not carry out some planned system enhancements, resulting in continued reliance on obsolete technology that hampered mission performance and made operations and maintenance more difficult and costly. The Coast Guard did not have plans in place to migrate to a common system baseline for the ships and aircraft included in the modernization project, which may result in higher life cycle costs and reduced mission effectiveness in the future. In several FY 2015 reports, GAO also discussed a lack of funding for acquisition of major Coast Guard assets.

The Coast Guard also did not have a routine process to ensure it maintained all fingerprints from aliens interdicted at sea in the Department's Automated Biometric Identification System. Poor system integration and failure to reconcile the biometric data, such as fingerprints, could impede identification of suspected terrorists, felons, or other individuals of interest. We identified some internal control weaknesses, including allowing employees to share passwords and not clearly defining system roles and responsibilities in the security plan. These weaknesses could result in individuals making unauthorized changes to the system without detection.

The Coast Guard faced challenges in protecting personally identifiable information and private information stored in IT systems and did not share consistent guidance for maintaining private information. The component lacked a strong organizational approach for safeguarding sensitive personally identifiable information and privacy data, such as protected health information. Coast Guard privacy and health officials did not formally communicate to improve privacy oversight and incident reporting, thereby limiting the Coast Guard's ability to assess and

mitigate the risks of future data breaches. The component did not have consistent instructions for managing and securing health records. Coast Guard clinics had also not completed contingency planning to safeguard privacy data from loss in case of disaster. Without an effective approach for resolving these privacy issues, Coast Guard personnel and their families risk the loss of privacy data and exposure to identity theft.

The Coast Guard agreed with our recommendations for addressing both these system implementation and data privacy and integrity issues. The Coast Guard is taking actions to resolve some of the issues identified, and complete resolution will likely not occur until the middle of FY 2016, including developing plans for safeguarding privacy data and periodically reviewing physical security of privacy data.

Moving Forward

IT plays a key role in supporting front-line operations, and having a vision and strategic objectives to meet the Department's goals is paramount. In releasing the *Department of Homeland Security Information Technology Strategic Plan FY 2015–2018*, DHS took a critical step toward achieving the most advanced, efficient, and effective management of IT and related services and resources. According to the DHS Chief Information Officer, the strategic plan is the coordinated effort to integrate people, processes, technology, information, and governance to fully support the needs of its workforce, partners, customers, and the American public, while addressing ever evolving mission challenges. The plan, developed collaboratively under the Secretary's Unity of Effort initiative, provides direction and guidance on advancing IT capabilities and resources to improve the Department's operational efficiency, mission effectiveness, and front-line operations. As a result, it positions DHS' technology environment to address the critical areas of people and culture, innovative technologies, cybersecurity, and governance and accountability.

Transportation Security

Effective coordination of people, processes, and technology is essential to protecting our transportation systems. The transportation security workforce must be properly vetted and well-trained, processes must be well-defined and modified when vulnerabilities are identified, and technology must aid the workforce in securing the Nation. Our recent work, including reviews of TSA's PreCheck initiative and the process to

vet aviation workers, as well as covert testing of airport passenger and baggage screening, shows that TSA continues to face challenges in all three areas.

Controlling access to secured airport areas is critical to the safety of passengers and aircraft. Although TSA makes efforts to ensure only cleared individuals enter secured areas, we identified several vulnerabilities. For example, we recently reported on TSA's PreCheck initiative, which provides expedited airport checkpoint screening for low-risk passengers at about 125 airports. Two of the four ways TSA selects passengers for expedited screening create security vulnerabilities. For instance, TSA granted a felon and former member of a domestic terrorist group expedited screening through TSA PreCheck. We concluded that TSA needs to modify the initiative's vetting and screening processes. Although TSA did not initially concur with all of our recommendations to correct deficiencies we identified with TSA PreCheck, it has made progress to implement the report's recommendations and address security vulnerabilities in the screening process.

We assessed TSA's controls over the vetting of aviation workers possessing or applying for credentials allowing unescorted access to secured airport areas. Although TSA's process for vetting workers was generally effective, TSA did not identify 73 individuals with possible terrorism-related category codes because current interagency watchlisting policy does not authorize TSA to receive all terrorism-related categories of information. Moreover, law and FBI policy generally prohibit TSA and the airports from conducting recurrent criminal history vetting for non-criminal justice purposes and rely on individuals to self-report disqualifying crimes. TSA is planning a pilot program for late 2015 whereby the FBI will begin providing automated updates for new criminal history matches associated with individuals who have undergone prior criminal history record checks.

The Department's Aviation Security Advisory Committee also reported on vulnerabilities within TSA's aviation vetting process. The Committee's Working Group on Airport Access Control released a report in April 2015 recommending airport employee vetting be strengthened by updating the list of disqualifying criminal offenses, continuous monitoring of criminal activity, and maintaining a national database of airport employees whose credentials have been revoked.[4]

---

[4]*Final Report of the Aviation Security Advisory Committee's Working Group on Airport Access Control*, April 8, 2015, www.tsa.gov

Through covert testing of airport passenger and baggage screening, we identified vulnerabilities caused by human, policy, and technology-based failures. DHS is taking steps to address these vulnerabilities. For instance, Secretary Johnson directed TSA to revise its standard operating procedures for screening and conduct training for all Transportation Security Officers (TSO) to address the specific vulnerabilities we identified.

Moving Forward

TSA cannot control all risks to transportation security, and unexpected threats will require TSA to improvise, but other issues are well within TSA's control. Sound planning and strategies for efficiently acquiring, using, and maintaining screening equipment that operates at full capability to detect dangerous items, for example, would improve overall operations. Better training and supervision of TSOs would help mitigate some effects of human errors. TSA's focus on its management practices and oversight of its technical assets and its workforce would help enhance security, as well as customer service, for passengers.

Border Security and Immigration Enforcement

DHS' components responsible for border security and immigration — CBP, ICE, U.S. Citizenship and Immigration Services (USCIS), and the Coast Guard — continue to face challenges due to the size and complexity of their varying missions. CBP apprehends more than 1,000 individuals each day for suspected violations of U.S. immigration laws. There are an estimated 11.5 million removable aliens in the United States, including people who may pose a risk to public safety or national security. Border security also encompasses the detection and interdiction of weapons of mass destruction, drugs, and other illicit goods; policies to combat human trafficking; and other security goals.

In FY 2015, we reported that CBP did not always effectively target rail shipments entering the United States from Canada and Mexico or consistently use the required radiation detection equipment to examine high-risk shipments. As a result of our report, CBP is drafting a comprehensive National Cargo Targeting Policy, which includes mandatory criteria for targeting rail shipments from Mexico and Canada. CBP is also ensuring that all rail ports have the required Radiation Isotope Identifier Devices to examine high-risk rail shipments and

documenting the results in its Cargo Enforcement Reporting and Tracking System.

Several of our FY 2015 reports demonstrate that DHS is hindered by a lack of data on immigration enforcement. Often, DHS cannot accurately assess program performance and make informed policy decisions because it either does not collect enough data to get a complete picture or the data it gathers is not reliable. For example:

- The Department does not collect or use the full range of prosecutorial discretion[5] data to help assess immigration policy, evaluate the effectiveness and results of enforcement actions, or assess the reasonableness of the exercise of prosecutorial discretion by DHS personnel.

- According to ICE, its Intensive Supervision Appearance Program (ISAP) is effective because few program participants abscond. However, ICE only measures whether aliens abscond or are arrested while they are actually participating in ISAP. Because ICE ends many aliens' participation in ISAP before their immigration cases are completed, it cannot definitively determine whether aliens who once were, but no longer are, in the program, have escaped or been arrested for criminal acts. ICE concurred with our recommendation to adjust program metrics and is working on a methodology to measure these "latent effects."

- ICE did not capture essential data, such as reasons detained aliens missed flights and the optimum seating capacity to support operational decisions related to air travel for detainees. For example, we determined that ICE did not always document whether detainees missed flights due to medical reasons or travel documentation problems. Without this information, ICE may miss opportunities to correct potential problems and improve the efficiency of its detainee air transportation program.

- CBP is not fully and accurately measuring Streamline's effect on deterring aliens from re-entering the country illegally. Streamline is an initiative to criminally prosecute individuals who illegally enter the U.S. through defined geographic regions. CBP measures Streamline's effect on re-entry using year-to-year data to analyze

---

[5] Prosecutorial discretion is the authority of an agency or officer to decide whether to enforce immigration laws, and if so, to what extent. For example, ICE enforcement officers are exercising prosecutorial discretion when deciding whom to stop, question, arrest, detain or remove from the country.

re-entry trends; it does not measure an alien's border crossing history, re-entry, or re-apprehension over multiple years. In other words, an alien who attempts to cross the border at the end of a fiscal year and makes a second attempt at the beginning of the next fiscal year would not be considered a recidivist. As a result of our report, CBP agreed to measure over multiple years and reported it is developing a State of the Border Risk Methodology Strategy to better assess and analyze its enforcement efforts.

Moving Forward

DHS plans to invest in a risk-based strategy for border security and a multi-pronged approach for assessing and accounting for its immigration enforcement efforts. Reporting all immigration enforcement actions would provide greater transparency and promote public confidence in the Department's immigration enforcement mission. Moreover, better data collection and analysis is essential to developing sound immigration and border security policies in the future.

Disaster Preparedness and Response

Ensuring the Nation is resilient to disasters requires strong coordination among the Department, first responders, citizens, and public and private sector partners. In our FY 2015 reports, we identified problems with internal controls, performance measures, and oversight of grants, which are key to the Department's ability to build, sustain, and improve the Nation's capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.

We reported that FEMA did not track costs or data associated with performance measures for Long Term Recovery Offices. Without tracking costs or data, FEMA could not determine whether these offices are cost effective. We found that FEMA establishes, operates, and closes Long Term Recovery Offices without standardized policies, procedures, and performance measures. Without these controls in place, FEMA risks mismanagement of Federal disaster funds and not ensuring consistency in establishing and managing these offices.

In our two FY 2015 audits of states' and urban areas' management of the Homeland Security Grant Program, we found states were challenged in developing state homeland security strategies and performance measures, obligating grant funds in a timely manner, accounting for and

spending grant funds, and monitoring subgrantees. In one audit, for example, because of insufficient management controls over subgrantees' use of funds and inadequate fiscal monitoring, we questioned $67 million that was either not spent in compliance with grant guidance or adequately supported. In another audit, the state had long-standing issues we had identified in two previous audits, but FEMA had not changed its oversight practices to target the repeated deficiencies and the state continued to disregard Federal regulations and grant guidance. As a result, that state may be limited in its ability to prevent, prepare for, protect against, and respond to major emergencies.

Many of our FY 2015 reports demonstrated the need for FEMA to better safeguard disaster assistance grant programs from fraud, waste, and abuse. For example, one report addressed the City of Biloxi, Mississippi's failure to follow Federal procurement standards for a $21.7 million contract. As a result, there was not always full and open competition, which increased the risk of fraud, waste, and abuse. Furthermore, at least $8.1 million of the $21.7 million in contract costs was unreasonable.

In September 2015, we issued our sixth annual capping report for disaster-related audits demonstrating the continued problems with grant management, ineligible and unsupported costs, and noncompliance with Federal contracting requirements. From FYs 2009 through 2014, we audited grant funds totaling $9.35 billion and reported potential monetary benefits — based on our questioned costs and recommendations — of $2.3 billion, or an average of 25 percent of the amount audited.

FEMA has taken our audit work seriously and continued to improve its ability to better steward taxpayers' money. For example, in response to our FY 2014 disaster assistance reports, FEMA took corrective actions to close 146 of our 159 recommendations. This included acting on our recommendation to collect a $29 million delinquent debt from Louisiana. As of April 30, 2015, Louisiana agreed to pay FEMA $53.8 million over 5 years for this debt and for other overpayments. Additionally, FEMA has collaborated with Louisiana to identify eligible use for more than $400 million in unobligated hazard mitigation funds. Unobligated Hazard Mitigation Grant Program funds represent missed or delayed opportunities to protect the lives and property of citizens from future disasters. During the last year, FEMA worked with Louisiana to identify and develop viable projects and FEMA continues to identify additional eligible work to further reduce Louisiana's amount of unobligated grant funds.

FEMA's Recovery Directorate established a Recovery Audits Section dedicated to overseeing, coordinating, responding to, and implementing our audit recommendations. Since launching the section in June 2014, FEMA has begun hiring staff; developing procedures to improve the quality and timeliness of audit responses; and identifying ways to improve audit-related information sharing, recordkeeping, and communication between FEMA Headquarters and Regional Recovery Divisions. FEMA anticipates the Recovery Audits Section will reach full staffing and operating capacity by the end of FY 2015.

Moving Forward

FEMA has worked to better prepare the Nation and enhance its ability to build, sustain, and improve response capabilities. FEMA must continue to strengthen oversight for both preparedness and disaster assistance grants to ensure grant programs achieve the intended objectives and deter fraud, waste, abuse, and noncompliance.

Infrastructure Protection and Cybersecurity

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. DHS must take a holistic approach to cybersecurity and infrastructure protection, including examination of people, processes, and technology involved in safeguarding critical assets and information. As a result of our FY 2015 cybersecurity and infrastructure protection audit projects, we identified a common need for better oversight, training, formal policies and processes, controls, and contingency planning.

Ensuring that the people with access and responsibility for managing critical assets and information are appropriately vetted and managed is of paramount importance in cybersecurity. The Coast Guard has taken steps to address the risk that employees with authorized access may pose to key information systems and data. These steps include establishing an insider threat program, verifying that system administrators have appropriate system access levels, and establishing a cybersecurity operations center to monitor and respond to potential insider threat risks. However, the Coast Guard could implement software to protect against unauthorized removal of sensitive information, implement stronger physical security controls, and provide insider threat security awareness training for all its employees.

Our annual *Federal Information Security Management Act* (FISMA) reports address both the processes and technologies needed to ensure cybersecurity. In December 2014, we issued our FY 2014 FISMA report in which we found that DHS had taken steps to improve the policies, procedures, and system security controls for enterprise-wide information security programs. These steps included enhancing its risk management approach; developing an information security performance plan; and implementing trusted internet connections, continuous monitoring, and strong authentication in line with the President's cybersecurity priorities. However, DHS components were not consistently updating the system inventory and plan of action and milestones in the Department's enterprise management systems. Components continued to operate systems without the proper authority. In addition, the Secret Service did not provide the DHS Chief Information Security Officer with continuous monitoring data as the Office of Management and Budget required.

Our FY 2014 FISMA review of the Department's enterprise-wide intelligence systems showed that the Office of Intelligence and Analysis (I&A) continued to effectively monitor DHS systems and security practices. For example, I&A had updated policies and procedures for managing sensitive compartmented information systems, and the Coast Guard had migrated its Intelligence Support System to a new system largely supported by the Defense Intelligence Agency. However, we identified deficiencies in I&A's configuration management and in the Coast Guard's continuous monitoring, configuration management, risk management, security training, and contingency planning.

External entities also raised concerns about the Federal Government's need to strengthen cybersecurity. For example, in June 2015, a RAND Corporation official testified before Congress that the Government needs to improve its ability to sense threats in real time and respond rapidly. Without a strong defensive capacity, our Nation may be more at risk of additional unauthorized network intrusions. According to the testimony, to mitigate this risk, two key components of DHS' defensive cyber capacity — Continuous Diagnostic Monitoring and EINSTEIN, a government-wide system managed by DHS — need additional resources and development. Specifically, continuous monitoring provides ongoing awareness of information security, vulnerabilities, and threats to support risk management decisions, and EINSTEIN is a system used to automatically detect malicious network activity and create alerts when triggered.

The Nation has directed increased attention toward physical protection of the 16 critical infrastructures spanning the U.S. economy.[6] Dialogue with the private sector and nationwide planning are crucial elements in coordinating an effective approach to safeguarding against natural and manmade events, including cyber-attacks. In FY 2015, GAO highlighted concerns in key infrastructure areas. For example, in July 2015, GAO suggested that DHS, in conjunction with the Department of Energy, needed to identify clear internal agency roles and responsibilities for addressing electromagnetic threats. Such threats, posed by an electromagnetic pulse or solar weather event, could lead to power outages over broad geographic areas for extended durations and could have debilitating impacts on the Nation's critical infrastructure.

GAO also reported the Department used unverified and self-reported data to categorize the risk of a toxic release from chemical facilities. In its report, GAO estimated that more than 2,700 of about 6,400 facilities with a toxic release threat misreported the distance of concern, or the area in which exposure to a toxic chemical cloud could cause serious injury or fatalities from short-term exposure. By verifying that the data used in its risk assessment is accurate, DHS could better ensure it has identified the Nation's high-risk chemical facilities.

The National Infrastructure Advisory Council, which advises the President through the DHS Secretary, stressed that managing these infrastructure risks will require greater integration of activities, and consideration of long-term as well as short-term investments, within and across sectors.

Moving Forward

The Department has recognized cybersecurity as a critically important part of its mission and is continuing to build an agile and responsive cybersecurity capability. DHS and its components have taken steps to implement our recommendations and address vulnerabilities identified. The Coast Guard agreed with our recommendations for addressing the risk of insider threats to its information systems and data. After completion of our fieldwork on the 2014 FISMA reports, the Secret Service reached agreement with the DHS Chief Information Officer to provide the required data in subsequent years.

---

[6] Critical infrastructure comprises physical and cyber systems and assets so vital to the United States that their incapacity or destruction would have a debilitating effect on national security, economic security, public health and safety, or any combination of those matters.

Employee Accountability and Integrity

To secure the Nation from the many threats we face, DHS depends on the integrity of Federal employees and contractors in jobs that range from aviation and border security to emergency response, from cybersecurity analyst to chemical facility inspector. Although the vast majority of DHS employees are honest and dedicated, the few who commit crimes or engage in other egregious misconduct can compromise the integrity of DHS' programs and operations, undermine the public's trust, and damage our national security. The Department's challenge is to be vigilant in deterring and taking action to stop such activities.

The Department has a large concentration of Federal law enforcement officers, including the Nation's largest police force, CBP, and the second largest investigative agency in the country, ICE. As an organization with a national security and law enforcement mission, CBP is vulnerable to the potential for corruption within its workforce. Transnational criminal organizations that operate on both sides of our borders have budgets in the tens of millions of dollar for bribes and corruption of government officials. Even the perception of widespread corruption may inhibit information sharing with other agencies and thus hinder effective border enforcement and interdiction.

We investigated a Border Patrol agent for money laundering and structuring $61,600 of mutilated cash into nine deposits to evade Federal reporting requirements. He was sentenced to imprisonment, followed by supervised release. He was also ordered to forfeit $28,100 and pay a fine of $9,720. Another Border Patrol agent, whose live-in girlfriend was allegedly assisting a drug trafficking organization, was involved in the illegal procurement and sale of firearms, sometimes to fellow agents.

We also investigated an Immigration Services Officer who accepted bribes of up to $5,000 in exchange for falsifying immigration documentation. After his arrest and while he was out on bond, he and his wife visited potential government witnesses and attempted to influence their upcoming testimony. He and his wife were both sentenced to incarceration to be followed by supervised release. We also investigated an Immigration Services Officer who was accepting bribes to approve immigration applications. The officer was terminated from employment and sentenced to incarceration and supervised release and ordered to pay a $6,000 fine.

We reviewed allegations that senior leadership officials at the Secret Service ordered a protection operation on behalf of an administrative employee after the employee was involved in a dispute with a neighbor. We found no specific statutory or regulatory authorization for the use of component resources to protect an employee who is involved in a private, non-work related dispute, and that the diverted Special Agents, whose primary duty was to patrol the area around the White House, would have been unable to respond to exigencies at the White House. The President was at the White House on two of the occasions the Special Agents were diverted to the protection operation.

In 2015, we also looked at the use of counterfeit funds. We investigated a Secret Service Special Agent who had improperly taken approximately $6,830 in counterfeit money. The Special Agent was sentenced to 9 months' incarceration to be followed by 12 months of supervised release and ordered to pay a $20,000 fine. In addition, we investigated an administrative officer who was stealing counterfeit Federal Reserve notes from a Secret Service office and using them at a local department store. Through executing search warrants, we seized thousands of dollars of counterfeit and legitimate U.S. currency. The administrative officer was sentenced to probation and home detention.

Moving Forward

The Department must continue to be diligent in deterring and taking action against fraud, waste, and abuse. Whistleblowers, by their willingness to step forward and identify problems, are crucial to these efforts. Whistleblower disclosures play a crucial role in keeping the Department efficient and accountable. To assist employees, DHS created a "Whisteblower Protection" page on its intranet website to consolidate information and address common questions employees who report or are considering reporting concerns may have. It also contains details on legal protections, guidance documents, and other resources.

Use-of-force policies, practices, and techniques are essential to the credibility of law enforcement agencies within the communities they serve. In FY 2014, in an effort to improve transparency, DHS for the first time publicly released the DHS-wide use-of-force policy, and CBP and ICE publicly released their use-of-force policies. CBP established a national Use of Force Review Board to review use-of-force incidents resulting in death or serious bodily injury. We expect the Use of Force Review Board to increase accountability and transparency, and we will continue to investigate and oversee certain use-of-force allegations and incidents.

Appendix A
Relevant Reports

DHS OIG reports can be found under the "Reports" tab at
http://www.oig.dhs.gov/

Introduction

- DHS, *DHS Budget-in-Brief*, Fiscal Year 2016.
  http://www.dhs.gov/sites/default/files/publications/FY_2016_DHS_Budget_in_Brief.pdf
- DHS, *The 2014 Quadrennial Homeland Security Review*, June 2014.
  http://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf

DHS Management and Operations Integration

- DHS-OIG, *Accurate Reporting and Oversight Needed to Help Manage DHS' Warehouse Portfolio*, (OIG-15-138, August 2015)
  https://www.oig.dhs.gov/assets/Mgmt/2015/OIG-15-138-Aug15.pdf
- DHS-OIG, *DHS Needs to Improve Grant Guidance for Public Safety Communications Equipment*, (OIG-15-124, August 2015)
  https://www.oig.dhs.gov/assets/Mgmt/2015/OIG-15-124-Aug15.pdf
- DHS-OIG, *Fiscal Year 2014 Assessment of DHS Charge Card Program Indicates Moderate Risk Remains*, (OIG-15-117, July 2015)
  https://www.oig.dhs.gov/assets/Mgmt/2015/OIG-15-117-Jul15.pdf
- DHS-OIG, *Corrective Actions Still Needed to Achieve Interoperable Communications*, (OIG-15-97-R, May 2015)
  https://www.oig.dhs.gov/assets/GrantReports/2015/OIG_15-97-VR_May15.pdf
- DHS-OIG, *DHS Should Do More to Reduce Travel Reservation Costs*, (OIG-15-80, April 2015)
  https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-80_Apr15.pdf

Acquisition Management

- DHS OIG, *The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program*, (OIG-15-86, May 2015)
  https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-86_May15.pdf
- DHS OIG, *DHS Contracts and Grants Awarded through Other than Full and Open Competition, FY 2014*, (OIG-15-59, April 2015)
  https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-59_Apr15.pdf

- DHS OIG, *CBP's Oversight of Its Non-Intrusive Inspection Equipment Maintenance Contracts Needs Improvement,* (OIG-15-53, March 2015) https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-53_Mar15.pdf
- DHS OIG, *Science and Technology Directorate Needs to Improve Its Contract Management Procedures,* (OIG-15-38, February 2015) https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-38_Feb15.pdf
- DHS OIG, *The United States Secret Service Has Adequate Oversight and Management of Its Acquisitions (Revised),* (OIG-15-21, February 2015) https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-21_Feb15.pdf
- DHS OIG, *U.S. Customs and Border Protection's Management of National Aviation Maintenance Activities, (No report number, January 2015)* https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_MngAdv15.pdf
- DHS OIG, *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) https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-17_Dec14.pdf

Financial Management

- DHS-OIG, *Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting,* (OIG-15-10, November 2014) https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-10_Nov14.pdf
- DHS-OIG, *Independent Auditors' Report on DHS' FY 2015 Financial Statements and Internal Control over Financial Reporting,* (OIG-16-06, November 2015) http://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-06-Nov15.pdf

Information Management and Technology

- DHS-OIG, *United States Coast Guard Safeguards for Protected Health Information Need Improvement,* (OIG-15-87, May 2015) https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-87_May15.pdf
- DHS-OIG, *The Security Posture of the United States Coast Guard's Biometrics At Sea System Needs Improvements,* (OIG-15-41, March 2015) https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-41_Mar15.pdf
- DHS-OIG, *U.S. Coast Guard Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance Modernization,* (OIG-15-05, October 2014) https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-05_Oct14.pdf
- DHS-OIG, *FEMA's Logistics Supply Chain Management System May Not Be Effective During a Catastrophic Disaster,* (OIG-14-151, September 2014) https://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-151_Sep14.pdf

- DHS-OIG, *Implementation Status of the Enhanced Cybersecurity Services Program*, (OIG-14-119, July 2014).
  http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-119_Jul14.pdf

Other Sources
- GAO, *Homeland Security Acquisitions: Major Program Assessments Reveal Actions Needed to Improve Accountability*, (GAO-15-171SP, April 2015)
  http://www.gao.gov/assets/670/669791.pdf
- GAO, *Facial Recognition: Commercial Uses, Privacy Issues, and Applicable Federal Law*, (GAO-15-621, July 2015)
  http://gao.gov/assets/680/671764.pdf
- GAO, *Coast Guard Acquisitions: As Major Assets Are Fielded, Overall Portfolio Remains Unaffordable*, (GAO-15-620T, May 2015)
  http://www.gao.gov/assets/680/670215.pdf
- GAO, *Coast Guard Acquisitions: Better Information on Performance and Funding Needed to Address Shortfalls*, (GAO-14-450, June 2014)
  http://gao.gov/assets/670/663881.pdf

Transportation Security

- DHS-OIG, *(U) Covert Testing of the Transportation Security Administration's Passenger Screening Technologies and Processes at Airport Security Checkpoints, Unclassified Summary*, (OIG-15-150, September 2015)
  https://www.oig.dhs.gov/assets/Mgmt/2015/OIG-15-150-Sep15.pdf
- DHS-OIG, *TSA Can Improve Aviation Worker Vetting (Redacted)*, (OIG-15-98, June 2015) https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-98_Jun15.pdf
- DHS-OIG, *Allegation of Granting Expedited Screening through TSA Pre✓® Improperly (OSC File No. DI-14-3679) (Redacted)*, (OIG-15-45, March 2015)
  https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-45_Mar15.pdf
- DHS-OIG, *(U) Security Enhancements Needed to the Pre✓® Initiative, Unclassified Summary*, (OIG-15-29, January 2015)
  https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-29_Feb15.pdf

Border Security and Immigration Enforcement

- DHS-OIG, *Streamline: Measuring Its Effect on Illegal Border Crossing*, (OIG-15-95, May 2015)
  https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-95_May15.pdf
- DHS-OIG, *DHS Missing Data Needed to Strengthen Its Immigration Enforcement Efforts*, (OIG-15-85, May 2015)
  https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-85_May15.pdf
- DHS-OIG, *ICE Air Transportation of Detainees Could Be More Effective*, (OIG-15-57, April 2015)

https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-57_Apr15.pdf

- DHS-OIG, *U.S. Customs and Border Protection Did Not Effectively Target and Examine Rail Shipments From Canada and Mexico*, (OIG-15-39, March 2015) https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-39_Mar15.pdf
- DHS-OIG, *U.S. Immigration and Customs Enforcement's Alternatives to Detention*, (OIG-15-22, February 2015) https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-22_Feb15.pdf

Disaster Preparedness and Response Management

- DHS-OIG, *Summary and Key Findings of Fiscal Year 2014 FEMA Disaster Grant and Program Audits*, (OIG-15-146-D, September 2015) https://www.oig.dhs.gov/assets/GrantReports/2015/OIG-15-146-D-Sep15.pdf
- DHS-OIG, *FEMA Should Recover $21.7 Million of $376 Million in Public Assistance Grant Funds Awarded to the City of Biloxi, Mississippi, for Hurricane Katrina Damages*, (OIG-15-131-D, August 2015) https://www.oig.dhs.gov/assets/GrantReports/2015/OIG-15-131-D-Aug15.pdf
- DHS-OIG, *FEMA Should Recover $9.3 Million of Ineligible and Unsupported Costs from Fox Waterway Agency in Fox Lake, Illinois*, (OIG-15-114-D, July 2015) https://www.oig.dhs.gov/assets/GrantReports/2015/OIG-15-114-D-Jul15.pdf
- DHS-OIG, *FEMA Should Disallow over $4 Million Awarded to Mountain View Electric Association, Colorado, for Improper Procurement Practices*, (OIG-15-113-D, July 2015) https://www.oig.dhs.gov/assets/GrantReports/2015/OIG-15-113-D-Jul15.pdf
- DHS-OIG, *FEMA Should Recover $4.85 Million of Ineligible Grant Funds Awarded to Oklahoma City, Oklahoma*, (OIG-15-111-D, July 2015) https://www.oig.dhs.gov/assets/GrantReports/2015/OIG-15-111-D-Jul15.pdf
- DHS-OIG, *Kansas and the Unified School District #473 in Chapman, Kansas, Did Not Properly Administer $50 Million of FEMA Grant Funds* (OIG-15-109-D, June 2015) https://www.oig.dhs.gov/assets/GrantReports/2015/OIG_15-109-D_Jun15.pdf
- DHS-OIG, *New York's Management of Homeland Security Grant Program Awards for Fiscal Years 2010–12*, (OIG-15-107, June 2015) https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-107_Jun15.pdf
- DHS-OIG, *FEMA Should Recover $337,135 of Ineligible or Unused Grant Funds Awarded to the Port of Tillamook Bay, Oregon* (OIG-15-104-D, June 2015)

https://www.oig.dhs.gov/assets/GrantReports/2015/OIG_15-104-D_Jun15.pdf

- DHS-OIG, *The Chippewa Cree Tribe of the Rocky Boy's Indian Reservation in Montana Mismanaged $3.9 Million in FEMA Disaster Grant Funds*, (OIG-15-101-D, June 2015)
  https://www.oig.dhs.gov/assets/GrantReports/2015/OIG_15-101-D_Jun15.pdf

- DHS-OIG, *Boulder County, Colorado, Has Adequate Policies and Procedures to Manage Its Grant, but FEMA Should Deobligate about $2.5 Million in Unneeded Funds,* (OIG-15-99-D, June 2015)
  https://www.oig.dhs.gov/assets/GrantReports/2015/OIG_15-99-D_Jun15.pdf

- DHS-OIG, *FEMA Should Recover $2.75 Million of $16.9 Million in Public Assistance Grant Funds Awarded to the Borough of Seaside Heights, New Jersey,* (OIG-15-90-D, May 2015)
  https://www.oig.dhs.gov/assets/GrantReports/2015/OIG_15-90-D_May15.pdf

- DHS-OIG, *FEMA Misapplied the Cost Estimating Format Resulting in an $8 Million Overfund to the Port of Tillamook Bay, Oregon,* (OIG-15-89-D, May 2015)
  https://www.oig.dhs.gov/assets/GrantReports/2015/OIG_15-89-D_May15.pdf

- DHS-OIG, *FEMA Should Disallow $82.4 Million of Improper Contracting Costs Awarded to Holy Cross School, New Orleans, Louisiana,* (OIG-15-65-D, April 2015)
  https://www.oig.dhs.gov/assets/GrantReports/2015/OIG_15-65-D_Apr15.pdf

- DHS-OIG, *Florida and the Palm Beach County School District Did Not Properly Administer $7.7 Million of FEMA Grant Funds Awarded for Hurricane Jeanne Damages,* (OIG-15-51-D, March 2015)
  https://www.oig.dhs.gov/assets/GrantReports/2015/OIG_15-51-D_Mar15.pdf

- DHS-OIG, *Florida and Palm Beach County School District Did Not Properly Administer $9.2 Million of FEMA Grant Funds Awarded for Hurricane Wilma Damages,* (OIG-15-50-D, March 2015)
  https://www.oig.dhs.gov/assets/GrantReports/2015/OIG_15-50-D_Mar15.pdf

- DHS-OIG, *FEMA Needs to Ensure the Cost Effectiveness of $945,640 that Los Angeles County, California Spent for Hazard Mitigation Under the Public Assistance Program,* (OIG-15-40-D, March 2015)
  https://www.oig.dhs.gov/assets/GrantReports/2015/OIG_15-40-D_Mar15.pdf

- DHS-OIG, *FEMA Should Recover $6.2 Million of Ineligible and Unused Grant Funds Awarded to the Imperial Irrigation District, California,* (OIG-15-35-D,

February 2015)
https://www.oig.dhs.gov/assets/GrantReports/2015/OIG_15-35-D_Feb15.pdf

- DHS-OIG, *FEMA Insurance Reviews of Applicants Receiving Public Assistance Grant Funds for 2004 and 2005 Florida Hurricanes Were Not Adequate,* (OIG-15-19-D, December 2014) https://www.oig.dhs.gov/assets/GrantReports/2015/OIG_15-19-D_Dec14.pdf

- *Needs To Track Performance Data and Develop Policies, Procedures, and Performance Measures for Long Term Recovery Offices*, (OIG-15-06-D, October 2014) https://www.oig.dhs.gov/assets/GrantReports/2015/OIG_15-06-D_Oct14.pdf

- DHS-OIG, *Ohio's Management of Homeland Security Grant Program Awards for Fiscal Years 2010 Through 2012* (Revised), (OIG-15-08, January 2015) https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-08_Jan15.pdf

- DHS-OIG, *The State of North Dakota Needs to Assist Ramsey County in Completing $24 Million of FEMA Public Assistance Projects for Three Federally Declared Disasters that Occurred in 2009–2011*, (OIG-15-03-D, October 2014) https://www.oig.dhs.gov/assets/GrantReports/2015/OIG_15-03-D_Oct14.pdf

- DHS-OIG, *FEMA Should Recover $3 Million of Ineligible Costs And $4.3 Million of Unneeded Funds from the Columbus Regional Hospital*, (OIG-15-02-D, October 2014) https://www.oig.dhs.gov/assets/GrantReports/2015/OIG_15-02-D_Oct14.pdf

- DHS-OIG, *FEMA Should Recover $13 Million of Grant Funds Awarded to The Administrators of the Tulane Educational Fund, New Orleans, Louisiana,* (OIG-15-01-D, October 2014) https://www.oig.dhs.gov/assets/GrantReports/2015/OIG_15-01-D_Oct14.pdf

- DHS-OIG, *FEMA and the State of Louisiana Need to Accelerate the Funding of $812 Million in Hazard Mitigation Grant Program Funds and Develop a Plan to Close Approved Projects*, (OIG-14-150-D, September 2014) https://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-150-D_Sep14.pdf

Employee Accountability and Integrity

- *DHS-OIG, Semi-Annual Report to the Congress, October 1, 2014 through March 31, 2015,* (April 30, 2015) https://www.oig.dhs.gov/assets/SAR/OIG_SAR_Oct01_Mar31.pdf

Infrastructure Protection and Cybersecurity

- DHS-OIG, *United States Coast Guard Has Taken Steps to Address Insider Threats, but Challenges Remain*, (OIG-15-55, March 2015)
  https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-55_Mar15.pdf
- DHS-OIG, *(U) Fiscal Year 2014 Evaluation of DHS' Compliance with Federal Information Security Management Act Requirements for Intelligence Systems, Unclassified Summary*, (OIG-15-33, February 2015)
  https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-33_Feb15.pdf
- DHS-OIG, *Evaluation of DHS' Information Security Program for Fiscal Year 2014*, (OIG-15-16, December 2014)
  https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-16_Dec14.pdf

Other Sources
- GAO, *Preliminary Observations on DHS Efforts to Address Electromagnetic Threats to the Electric Grid*, (GAO-15-692T, July 2015)
  http://www.gao.gov/assets/680/671554.pdf
- GAO, *Critical Infrastructure Protection: DHS Action Needed to Verify Some Chemical Facility Information and Manage Compliance Process,* (GAO-15-614, July 2015)
  http://www.gao.gov/assets/680/671570.pdf
- Daniel Gerstein, RAND Corporation, *Strategies for Defending U.S. Government Networks in Cyberspace, before the House Homeland Security Committee, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies*, June 2015
  http://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT436/RAND_CT436.pdf
- National Infrastructure Advisory Council, *Executive Collaboration for the Nation's Strategic Critical Infrastructure*, March 2015
  http://www.dhs.gov/sites/default/files/publications/NIAC-CEO-Final-Report-QBM-Draft-508.pdf

Appendix B
DHS Comments to the Draft Report

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

November 10, 2015

MEMORANDUM FOR: The Honorable John Roth
Inspector General
Office of Inspector General

FROM: Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

SUBJECT: Draft Report OIG-16-07, "Major Management and Performance
Challenges Facing the Department of Homeland Security"
(Project No. 15-064-AUD-MGMT)

Thank you for the opportunity to review and comment on this draft report. The U.S.
Department of Homeland Security (DHS) appreciates having the Office of Inspector
General (OIG) perspective on the most serious management and performance challenges
facing the Department.

DHS agrees with OIG's assessment, that "the Department's strongest asset [is] its
people." As Secretary of Homeland Security Jeh Johnson stated in his testimony before
Congress earlier this year, "… maintaining the security of our homeland is made possible
through the dedicated work of the nearly quarter million men and women who comprise
DHS." The Department's leadership priorities are focused on our mission of ensuring a
homeland that is safe, secure, and resilient against terrorism and other hazards. We strive
to implement programs that create opportunities for our employees to efficiently and
effectively achieve the strategies, goals, and objectives that this mission commands.

Secretary Johnson framed his Unity of Effort initiative by creating clear expectations for
collaboration for our workforce across the Department. Launched in 2014, the Unity of
Effort initiative serves as a driving force behind much of our daily operations and
activities. One year later, the initiative has resulted in building:
(1) important linkages between the Department's planning, programming,
budgeting, and execution processes;
(2) an approach to ensure that DHS invests and operates in a cohesive, unified
fashion; and,
(3) new forums in which enterprise-wide decisions are developed in a transparent
and collaborative process to drive strategic guidance to results.

DHS has achieved success by strengthening its existing business processes and developing new processes where needed, and we remain committed to building more success in coming years.

It is important to note that DHS missions are complex and highly diverse, sometimes requiring sustained management attention over a number of years in order to succeed in the improvement of program and operational effectiveness and efficiency. Given DHS's resource and budget constraints, it is even more important for the Department to improve its collective operation in order to more effectively and efficiently secure the homeland. This is true in both OIG's highlighted areas, as well as other parts of the DHS mission. DHS remains committed to improving those areas and needs as highlighted in this year's OIG management and performance challenges report.

For example, as recognized in your report, DHS has made great strides in closing OIG audit recommendations. Over the last few years, DHS and its Components steadily reduced the number of open recommendations by 65 percent from a high of 1,663 in FY 2011 to 583 in FY 2015.
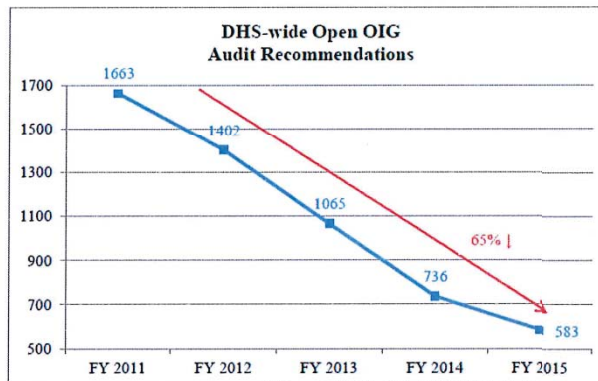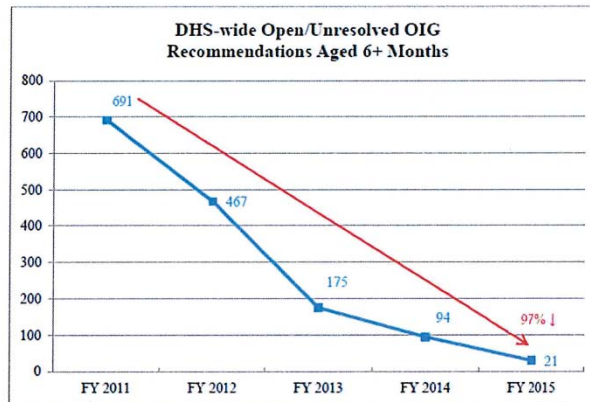

Even more significantly, the number of unresolved, open recommendations (i.e., those with disagreements) that are more than 6 months old have been reduced by 97 percent from a high of 691 in FY 2011 to 21 in FY 2015.

2

**DHS-wide Open/Unresolved OIG
Recommendations Aged 6+ Months**

```
800
        691
700
600
500
                    467
400
300                              175
200                                          94      97% ↓
100                                                          21
  0
      FY 2011    FY 2012      FY 2013     FY 2014    FY 2015
```

Audit follow-up is an integral part of good management and taking corrective action on unresolved findings and recommendations is essential to improving the effectiveness and efficiency of DHS activities. We appreciate the OIG's understanding that this is a shared responsibility of agency management officials and auditors. DHS recognizes that the aforementioned successes would not have been possible without the OIG leadership's willingness to work together with our program officials and others, as appropriate.

Additional examples of success and accomplishment related to the OIG's reported challenge areas are shown below:

Challenge #1: DHS Management and Operations Integration

The Unity of Effort initiative has accelerated the Management Directorate's efforts to accomplish the U.S. Government Accountability Office (GAO)- and OIG-suggested improvements by building a stronger management framework much earlier in the investment life cycle. DHS has matured the Unity of Effort initiative, and emphasized the need to improve acquisition management through enhancements to policies, structures and processes. The DHS Senior Leaders Council and the Deputy's Management Action Group, established by the initiative have been making strategy and resourcing decisions and have continued to oversee acquisition investments from the mission needs phase through completion of a program.

In the past year, these senior leader forums have made critical strategy, resource allocation, requirements, and operational planning decisions. The decisions have produced a leaner, more mission-focused FY 2016 budget, a campaign plan for the Southern Border and Approaches, the launch of three pilot joint task forces (JTF) to unify operations, and, the re-establishment of the Joint Requirements Council (JRC) to improve

3

the quality and validity of the Department's requirements validation and oversight process, as well as other significant effectiveness and efficiency enhancements.

The development and implementation of the DHS Communications Interoperability Plan serves as a formidable example of how DHS has improved governance, oversight, and collaboration on a program that crosses Component lines. The plan, signed in September 2015, establishes a decision-making body and a roadmap to improve tactical communications interoperability. In support of the plan, the Joint Wireless Program Management Office is refining implementation activities, while the Joint Wireless Program Executive Steering Committee focuses on interoperability matters. The increased Departmental oversight and governance, when combined with technology advancements in wireless communications, will enable DHS to better communicate with its law enforcement and public safety partners and increase operational effectiveness.

DHS's commitment to sustained management attention to GAO- and OIG-suggested improvements is evident in the Department's performance closing audit recommendations. For the fifth year in a row, DHS has sustained overall compliance with Office of Management and Budget (OMB)-mandated "A-50" audit follow-up and resolution requirements, and continued to close more recommendations than auditors have issued. An important goal in this area is to have no more than 20 percent of recommendations aged more than two years. DHS experienced particular success in moving closer to this goal for OIG recommendations during FY 2015, improving from 39 percent to 24 percent.

Challenge #2: Acquisition Management

The DHS Office of Program Accountability and Risk Management (PARM) provides the Department's central oversight of acquisition program management, including managing program governance, program support, and acquisition program management policy. In an effort to further strengthen oversight, the Secretary's Unity of Effort initiative is enhancing the coordination of Departmental planning, programming, budgeting, and execution processes through strengthened requirements processes and decision making, notably between the JRC and Acquisition Review Boards (ARBs).

The Department has expanded the oversight authority and scope of the ARB to focus on major issues beyond program performance and effectiveness. This approach helps to ensure that DHS remains a good steward of taxpayer dollars. For example, the ARB directed a U.S. Customs and Border Protection (CBP) specific Strategic Air and Marine Plan be reassessed within the context of the JRC's work on DHS Aviation Commonality and other emerging Unity of Effort initiatives. PARM has continued to work with Components to prepare for ARBs and schedule them when programs are ready for an acquisition decision event. In FY 2015, 26 action-oriented ARBs were held to provide oversight to DHS programs, more than double the number of ARBs held in FY 2014.

4

Several Components have improved their acquisition processes and taken steps to improve major acquisition programs. For example, the United States Secret Service (USSS) continues to improve its acquisition practices through partnerships with management, collaboration with the Resource Allocation Plan process, and support of existing and new programs. USSS has made significant efforts to identify and develop the acquisition workforce which has resulted in an increase in the number of certified personnel. USSS's Acquisition Management Program provides individual guidance and recommendations to help employees attain certifications in acquisition specialties.

Also, the Deputy Undersecretary for Management and the Transportation Security Administration's (TSA) leaders worked diligently to implement DHS Acquisition Policy and commercial best practices on the Electronic Baggage Screening Program. These efforts have yielded cost reductions through FY 2030 without negatively impacting the quality and effectiveness of the technology. In April 2015, GAO verified that TSA's screening program is on track to meet schedule and cost estimates.

In addition, an ARB identified that the Federal Emergency Management Agency's (FEMA's) Logistics Supply Chain Management System (LSCMS) risked not meeting desired requirements and running behind schedule. As a result, the Department paused the program. Through enhanced internal oversight and a joint effort between FEMA and the Management lines of business, the program is now back on track to meet requirements within the original estimated cost. TSA's Technology Infrastructure Modernization program was also suspended while the Component re-baselined the Surface and Aviation segments and updated acquisition documentation and strategy. In October 2015, the Chief Information Officer was directed to conduct an assessment of the TSA proposed strategy before the next ARB is held. This increased oversight ensures that programs are reviewed as they prepare to rebaseline and reenter the acquisition life cycle.

Challenge #3: Financial Management

DHS continues to build on its past two years of successful unmodified (clean) audit opinions by earning a third consecutive clean opinion on all financial statements. This achievement demonstrates DHS's sustained financial management progress and reflects the hard work of the men and women of this Department and the solid foundation of financial policies, processes and internal controls developed. DHS recognizes that additional improvements are possible and is working to achieve the goal of obtaining a clean opinion on internal control over financial reporting. DHS remains committed to the highest standard of accountability, transparency, and stewardship of taxpayer dollars.

As the third largest agency in the Federal Government, DHS is responsible for an annual budget of more than $60 billion. The entire DHS financial management community

5

continues to make progress in the shared responsibility to deliver effective financial management services despite new issues and challenges each year. For example, in FY 2015 DHS made significant progress in reducing the budgetary accounting material weakness. The DHS Chief Financial Officer partnered with the DHS Chief Procurement Officer to expedite contract closeouts. FEMA, U.S. Immigration and Customs Enforcement (ICE), and U.S. Coast Guard (USCG) strengthened their processes for timely deobligation of undelivered orders. These successes resulted in the Department's independent auditor downgrading last year's budgetary accounting material weakness to a significant deficiency. Additionally, USSS and CBP cleared audit conditions in the areas of financial reporting and property, plant and equipment, respectively. These improvements bring DHS closer to its goal of obtaining an unqualified (clean) audit opinion on internal control over financial reporting.

For the fourth consecutive year, DHS was able to provide a qualified assurance that its internal controls over financial reporting were operating effectively. The Department has established manageable, sustainable, and auditable processes for reporting the Statement of Budgetary Resources, allowing remediation this long-standing material weakness. There are three remaining weaknesses: Information Technology (IT) Controls and System Functionality; Property, Plant and Equipment; and Financial Reporting. DHS is committed to eliminating these material weaknesses to achieve a clean audit opinion on internal control over financial reporting.

In FY 2015, DHS implemented an independent verification and validation (IV&V) capability to provide oversight for test results that confirmed the remediation taken by Components was designed and operating effectively. To build on this progress, the Department will continue the ongoing remediation efforts and implement the risk based routine monitoring strategy that will test key internal controls appropriately across all significant business processes at the consolidated level.

The Department is making progress in financial systems modernization. In the first quarter of FY 2015, the Federal Law Enforcement Training Center's financial system underwent a technical refresh which corrected performance issues. The Domestic Nuclear Detection Office migrated to a Federal Shared Service Provider in the first quarter of FY 2016, with TSA and USCG lined up to go next. The Management Directorate, Science and Technology, U.S. Customs and Immigration Services, and the National Protection & Programs Directorate (NPPD) have completed their alternatives analyses and will be beginning systems modernization efforts in FY 2016. The Department has also initiated an IV&V review process to monitor our progress in real-time, in order to identify lessons to improve future modernization efforts.

While modernization efforts proceed, DHS continues to maximize legacy infrastructure and improve efficiency where possible. For example in FY 2015, DHS automated the generation of its monthly execution report to Congress. Previously a manual process, the

6

automation of the report saves considerable staff time each month and reduces the risk of errors. These efforts go toward ensuring DHS senior leadership and other stakeholders, including Congress, have current, accurate, and useful financial information to support decision making and oversight of the homeland security mission areas.

Challenge #4: Information Management and Technology

The Department has sustained the improvements made during FY 2014 and enhanced IT and management practices through implementation of the Administration's priorities. For example, to strengthen cybersecurity, the DHS Office of the Chief Information Security Officer has driven improvements Department-wide through the FY 2015 DHS Annual Information Security Performance Plan, and as a result, DHS achieved a 92 percent compliance rating for continuous monitoring on the "Federal Information Security Management Act" (FISMA) Cross Agency Priority Goals. Additionally, the Department expanded aggressive implementation of the Homeland Security Presidential Directive 12 Smartcard usage for logical access (login capability) to DHS unclassified networks which is required to increase the assurance that users are authorized to access DHS networks. As a result of OMB's government-wide 30-day sprint, DHS has over 95 percent unprivileged and over 99 percent privileged DHS Federal and contract staff Smartcard users nationwide. DHS exceeded OMB's FY 2015 goal for general users by 20 percent.

FEMA's LSCMS program office has satisfied all of the 2014 DHS Acquisitions Decision Memorandum requirements from the DHS Under Secretary for Management (USM) which had paused the LSCMS program. In addition, the LSCMS program office completed a limited analysis of alternatives, which reinforced that LSCMS is the preferred solution, and identified capability gaps which the program office had already began working on prior to the USM pause, including Electronic Data Interchange. In the interim, the program office deployed a capability known as Vendor Portal, which allows governmental agencies and strategic partners to fulfill orders for life saving commodities. In October 2015, the program office participated in the FEMA 2015 ARB and received DHS's support to re-baseline and resume the program upon the completion of certain action items, documentation, and improved software security to meet security requirements. Following resumption, the program office will work to close the capability gaps identified in the analysis of alternatives, and plans to return for an acquisition decision event no later than the first quarter of FY 2019 upon the completion of the operational test report.

USCG has also made progress on protecting personally identifiable information by establishing a formal mechanism to ensure communication between the USCG Privacy Officer and the Health Insurance Portability and Accountability Privacy and Security Official for enhanced privacy oversight and reporting. Moreover, USCG released an announcement to all USCG personnel in June 2015 to provide consistent instructions for

7

retaining and disposing health records. USCG is on track to fully implement additional protection measures by February 2016.

USCG has also improved efforts to protect other private information. For example, USCG has fully implemented all corrective actions to resolve deficiencies identified by DHS OIG to ensure that it maintains all fingerprints from aliens interdicted at sea in the Department's Automated Biometric Identification System. More specifically, USCG has implemented procedures to ensure that all data from USCG cutters capable of performing mobile 10-fingerprint biometrics collection at sea have been captured in this system.

In addition, USCG made progress on planning and implementation of mission-critical systems by implementing the Department of Defense-mandated Host Based Security System (HBSS). HBSS monitors every USCG system and alerts the USCG Cyber Command Security Operations Center upon detecting unauthorized or illegal universal serial bus connections to USCG systems. This provides protection again unauthorized connection of removal media devices and blocks communication between such devices and the USCG system to prevent unauthorized removal of information.

Challenge #5: Transportation Security

TSA's immediate priority is to determine root causes and implement solutions to address the recent covert testing of TSA's checkpoint operations and technology by OIG. TSA has undertaken a number of measures to accomplish Secretary Johnson's 10 point action plan addressed towards OIG's findings.

TSA is now working aggressively to accomplish these actions. The plan include:
(1) briefing all Federal security directors at airports nationwide on the OIG's preliminary test results to ensure leadership awareness and accountability which was completed in May and continues regularly;
(2) training every transportation security officer and supervisor to address the specific vulnerabilities identified by the OIG tests which began May 29, 2015 and was completed at the end of September 2015;
(3) increasing manual screening measures, including reintroducing hand-held metal detectors to resolve alarms at the checkpoint and reinforces our ability to detect the full range of threats;
(4) increasing the use of random explosives trace detection, enhancing detection capabilities to a range of threat vectors;
(5) re-testing and re-evaluating screening equipment to measure current performance standards—this testing, which began in June 2015 and is ongoing, will help us to more fully understand and strengthen equipment performance across the enterprise;
(6) assessing areas where screening technology equipment can be enhanced; and

8

(7) evaluating the current practice of including non-vetted populations in expedited screening.

TSA is exploring and reviewing expedited screening concepts with the intent of moving away from including non-vetted travelers into expedited screening lanes. Today, more than 6.5 million passengers are pre-vetted and travel with Known Traveler Numbers (KTNs). TSA is pursuing multiple avenues including adding marketing and enrollment opportunities to grow the population of fully-vetted travelers via programs such as TSA Pre✓® Application program or other DHS trusted traveler programs. TSA recently released a Request for Proposal which we believe will provide us with easier to use and more secure enrollment solutions using innovative technologies and processes. It is anticipated that these solutions will be in place during 2016. As an increasing number of travelers obtain KTNs, TSA has adjusted the manner in which travelers receive TSA Pre✓® expedited screening.

In March 2015, TSA began reducing the frequency in which travelers without KTNs, including those who previously opted-in via a frequent flyer program, were given TSA Pre✓® on their boarding passes. TSA is actively encouraging travelers to apply to the TSA Pre✓® Application Program by increasing visibility to the program through aggressive marketing and increasing enrollment capabilities through new business relationships with enrollment partners and travel management companies. This will increase the number of known low-risk travelers receiving TSA Pre✓® benefits. TSA has also recently eliminated the practice of using a combination of Behavior Detection Officers and explosive trace detection sampling to direct certain passengers into TSA Pre✓® expedited screening lanes, a practice known as "Managed Inclusion II."

Furthermore, TSA has undertaken the Standard Operating Procedures (SOP) Transformation Initiative to standardize, update, and streamline SOPs and provide the screening workforce with powerful tools to enhance effectiveness and increase compliance with procedures. Under the SOP Transformation Initiative, the information in 14 current security screening SOPs and their related interim changes have been issued in six transformed SOPs and one new SOP for screening policies. As TSA continues to implement these measures and other items included within the Secretary's action plan, TSA and DHS will continue to monitor implementation of these measures and will continue covert testing to assess the effectiveness of these actions.

Based on actions directed by Secretary Johnson and in alignment with recommendations from the Aviation Security Advisory Council (ASAC), TSA issued an update to its security directives requiring periodic renewal for the fingerprint-based Criminal History Records Check for aviation workers with existing airport-issued identification. Additionally, TSA is working to implement an FBI Rap Back pilot proof of concept by the end of this year, as well as implementing a number of the ASAC and OIG audit

9

recommendations to improve aviation security. Transportation Security Inspectors will inspect for compliance with these requirements regularly.

Challenge #6: Border Security and Immigration Enforcement

DHS continues to make the security of the Southern Border and Approaches a top priority. The Southern Border and Approaches Campaign Plan (Campaign) allows the Department to use its assets and personnel in a strategic and coordinated way across six lines of effort: reduce the terrorism risk to the nation; combat transnational criminal organizations; prevent exploitation of legal flows at ports of entry; counter illegal flows at maritime approaches and between ports of entry; manage lawful flows of people and goods in transit; and dis-incentivize illegal border behavior. The DHS JTFs, created to coordinate priorities and synchronize capabilities, became fully operational in FY 2015. The JTFs will continue to develop detailed operational plans, strengthen existing authorities and relationships, and coordinate Department-wide capabilities.

DHS border security performance management has taken several significant steps forward in FY 2015. The Department undertook a significant outcome-focused border security metrics exploration that is already providing new insight into the effects of certain border security policies, processes, and procedures. Expansion of this effort in FY 2016 will allow DHS to gain greater understanding of the impact of specific investments in people and equipment on DHS border security outcomes.

The U.S. Border Patrol has expanded its metrics and statistics efforts, including the ability to analyze recidivism data from the inception of Enforcement Systems to present. These methods and metrics are used by the Border Patrol to assess and adjust its tactical and operational effectiveness.

During the past year, DHS has taken steps to rebuild the Office of Immigration Statistics and implement Secretary Johnson's November 20, 2014, memorandum titled "Policies for the Apprehension, Detention, and Removal of Undocumented Immigrants" in an effort to better assess and analyze the array of immigration data that spans the Components.

ICE established metrics to evaluate the effectiveness and programmatic success of the Alternatives to Detention program. ICE is continuing to assess existing data and data collection methods with a view to more specifically identify challenges that need to be overcome before such a methodology can be put into place. After the initial evaluation, ICE will develop one or more performance metrics to gauge the effects of participation in alternatives to detention program on an individual's compliance with ICE reporting and court appearance requirements.

10

ICE is also working to develop metrics for performance management and modernizing systems to track and monitor operations and efficiencies across ICE Air Operations (IAO). During the past year, ICE IAO, under new leadership, has made noteworthy strides towards improving various staffing, training, data integrity, management, and systems modernization concerns, following a major consolidation and transition period. Numerous modernization projects have been initiated, and ICE IAO is coordinating with ICE Enforcement and Removal Operations programs to develop a strategic plan.

Challenge #7: Disaster Preparedness and Response

FEMA stands committed to identifying, tracking, and reporting the costs and performance data to show cost effectiveness for Long Term Recovery Offices. During the last year, FEMA has defined various models for post-disaster coordination and delivery of assistance. The agency has created an Integrated Planning Team to improve efficiency and effectiveness while developing and launching an Automated Common Operating Picture dashboard that identifies, tracks, and reports progress of disaster recovery and mitigation grants. In addition, FEMA is developing a strategic management plan to report staffing and administrative costs associated with Hurricane Sandy.

FEMA has also taken several steps to improve its disaster response and recovery capabilities. This includes the improvement of the Public Assistance Program delivery process, revising the grantee quarterly reporting process for Public Assistance and Hazard Mitigation Grant Program grants that improves visibility of individual projects, and establishing the Procurement Disaster Assistance Team capability to educate grantees and applicants regarding federal procurement under grants standards. Finally, the Recovery Audits Section reached full staffing and operating capacity during FY 2015.

Challenge #8: Infrastructure Protection and Cybersecurity

DHS has improved the strategic approaches, processes and technology needed to strengthen cybersecurity and protect critical infrastructure. For example, DHS is making progress toward full implementation of EINSTEIN 3 Accelerated (E3A). As of September 2015, E3A service is operational at two Internet service providers and protecting approximately 47 percent of the federal government. Service is scheduled to be operational at a third Internet service provider in the first quarter of FY 2016. Continuous Diagnostics and Mitigation (CDM), another key defensive cyber capacity initiative, received approval to hire 15 additional personnel in FY 2016 which will improve delivery of system capabilities to participating agencies. In addition, DHS is conducting research and analysis to better characterize electromagnetic pulse threats to critical infrastructure and to determine the most cost-effective solutions to these threats. FEMA has also begun developing a long-term power outage incident annex to the Response Federal Interagency Operational Plan to address the cascading impacts of electrical grid damage to other infrastructure systems. NPPD has begun developing a

11

process that will eliminate the need for chemical facilities to calculate and self-report distances of concern.

DHS Components have made progress ensuring that people with access and responsibility for managing critical assets and information are appropriately vetted and managed by undertaking several major initiatives. First, USCG fully implemented its Host Based Security System procedures which will provide responsible personnel with mechanisms to prevent, detect, and remediate malicious computer related activities and incidents. In addition, USCG provided its employees with insider threat training. Finally, USSS has improved personal identity verification card mandatory compliance for privileged access accounts.

DHS has also initiated efforts to take a more holistic approach to cybersecurity by improving guidance on safeguarding critical assets and information. The Office of the Chief Information Officer is leading this "defense in depth approach" to enhance the cybersecurity posture of our systems. DHS issued recent guidance and marketing materials to employees on how to best protect personally identifiable information and electromagnetic pulse protection guidelines for federal, state, and local partners. DHS has also improved compliance efforts to strengthen cyber defenses. For example, the DHS USM engaged Component heads to commit to action plans to address noncompliant cybersecurity measures. DHS also established a scorecard to assess DHS National Security Systems' compliance with FISMA and security continuous monitoring. Moreover, USSS has made considerable progress concerning overall FISMA and CDM monitoring by improving management of hardware assets, software assets, configuration, and information security vulnerabilities.

Challenge #9: Employee Accountability and Integrity

DHS works to deter or detect corruption and misconduct and to promote workforce integrity and accountability. Notably, CBP has made significant advancements during the past year in addressing corruption, misconduct, and use of force incidents. In September 2014, CBP announced the Integrity and Personal Accountability Strategy (Integrity Strategy) which serves as a comprehensive and multi-layered approach to preventing, detecting and investigating employee corruption and misconduct. The Integrity Strategy also addresses two primary cross-cutting strategic issues that span all mission areas: integration and awareness. It is intended to serve as a tool to unite CBP's independent office efforts under a single, unified mission to strengthen CBP's culture of integrity. Throughout every step in this strategic framework, enhancing employee awareness is a critical underpinning to successfully strengthening the CBP culture of integrity. Awareness is increased by training and communication programs that ingrain and reinforce the standards of conduct all employees are expected to maintain.

CBP also established a use of force protocol during FY 2015 which is a measured,

12

agency-wide process for investigating and reviewing use of force incidents. Designed to promote accountability and transparency of law enforcement within the communities served, the protocol includes specially trained, cross-Component use of force incident teams (UFITs) and use of force review boards (UFRBs). Under the new protocol, CBP immediately dispatches a UFIT to the scene to document the facts and circumstances surrounding a use of force event involving serious injury or death. Following refusal of criminal prosecution, the UFIT presents its findings to a National UFRB (NUFRB), comprised of senior managers from CBP's operational, legal, scientific, and training components as well as representatives from OIG, the DHS Office for Civil Rights and Civil Liberties, and the Department of Justice Civil Rights Division. The NUFRB determines if the use of force was consistent with CBP policy and makes findings and recommendations regarding any issues related to tactics, training, policy and equipment. CBP will publicly release final agency determinations and approved recommendations pertaining to use of force cases in accordance with applicable privacy laws.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. A short summary of the challenges and management response to the issues identified will be included in the Department's FY 2015 Agency Financial Report[1], as required by law. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

---

[1] http://www.dhs.gov/performance-accountability

13

Appendix C
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Chief Financial Officer
Chief Information Officer
Chief Security Officer
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.

OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305