

OFFICE OF INSPECTOR GENERAL

**Major Management and
Performance Challenges
Facing the Department of
Homeland Security (Revised)**



Homeland
Security

February 23, 2015
OIG-15-09



HIGHLIGHTS

Major Management and Performance Challenges Facing the Department of Homeland Security

February 23, 2015

Why We Did This

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

What We Recommend

We did not make any recommendations to the Department.

For Further Information:

Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

We have identified major challenges that affect both the Department as a whole, as well as individual components. DHS must continually seek to integrate management operations under an authoritative governing structure capable of effectively overseeing and managing programs that cross component lines.

DHS' mission to protect the Nation from domestic and international threats and respond to natural and manmade disasters is further challenged by the unpredictable nature of these hazards. DHS must overcome the challenges inherent with uniting the Department under the Secretary's Unity of Effort Initiative, as well as those over which it has little control.

This year, we are reporting the Department's major challenges in the following areas:

- DHS Operations Integration
- Acquisition Management
- Financial Management
- IT Management and Privacy Issues
- Transportation Security
- Border Security and Immigration Enforcement
- Grants Management
- Employee Accountability and Integrity
- Infrastructure Protection, Cybersecurity, and Insider Threat



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

February 23, 2015

MEMORANDUM FOR: The Honorable Jeh Johnson
Secretary

FROM: John Roth *John Roth*
Inspector General

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

Attached for your information is our revised annual report, *Major Management and Performance Challenges Facing the Department of Homeland Security, OIG-15-09*. We reissued the report with a correction to the Employee Accountability and Integrity, FY 2014 Observations section on page 16. Please see the attached errata for details.

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

Attachment

Errata page for OIG-15-09

Major Management and Performance Challenges Facing the Department of Homeland Security

**Change made to the Employee Accountability and Integrity,
FY 2014 Observations section, page 16, 1st paragraph (see below):**

Changed from:

In FY 2014, we have received approximately 29,000 complaints and opened more than 1,000 investigations. In that same period, approximately 200 cases were accepted for prosecution. We have achieved 300 convictions and effected 100 personnel actions.

Changed to:

In FY 2014, we have received approximately 16,281 complaints and opened more than 500 investigations. In that same period, approximately 100 cases were accepted for prosecution. We have achieved 112 convictions and effected 36 personnel actions.



Major Management and Performance Challenges Facing the Department of Homeland Security

The attached report presents our fiscal year (FY) 2014 assessment of the major management and performance challenges facing the Department of Homeland Security (DHS). As required by the *Reports Consolidation Act of 2000* (Public Law 106-531), we update our assessment of management challenges annually. As stipulated, the report summarizes what the Office of Inspector General (OIG) considers to be the most serious management and performance challenges facing the agency and briefly assesses the agency's progress in addressing those challenges.

We have identified major challenges that affect both the Department as a whole, as well as individual components. Some of the most persistent challenges arise from the effort to combine and coordinate diverse legacy agencies into a single, cohesive organization capable of fulfilling a broad, vital, and complex mission. DHS must continually seek to integrate management operations under an authoritative governing structure capable of effectively overseeing and managing programs that cross component lines.

DHS' mission to protect the Nation from domestic and international threats and respond to natural and manmade disasters is further challenged by the unpredictable nature of these hazards. DHS must overcome the challenges inherent with uniting the Department under the Secretary's Unity of Effort Initiative, as well as those over which it has little control.

This year, we are reporting the Department's major challenges in the following areas:

- DHS Operations Integration
- Acquisition Management
- Financial Management
- IT Management and Privacy Issues
- Transportation Security
- Border Security and Immigration Enforcement
- Grants Management
- Employee Accountability and Integrity
- Infrastructure Protection, Cybersecurity, and Insider Threat



Background

In *The 2014 Quadrennial Homeland Security Review* (2014 QHSR), DHS envisaged a homeland that is safe, secure, and resilient against terrorism and other hazards, where American interests, aspirations, and way of life can thrive. The Department also reported it would continue to adhere to the five basic homeland security missions set forth in the first QHSR, issued in 2010, but that it would refine these missions to reflect the evolving landscape of homeland security threats and hazards. To accomplish this vision, the 2014 QHSR identified the following 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; and
5. Strengthen national preparedness and resilience.

Although DHS' FY 2014 budget was about \$60 billion, resource constraints necessitate greater unity of effort and should motivate DHS to mature into an entity that is greater than the sum of its parts. Accomplishing these missions requires coordination across all DHS activities and among numerous homeland security partners and stakeholders. The five missions advance each of the four enduring national interests articulated in the *National Security Strategy*. Successful accomplishment of these missions results in a secure homeland, fosters a thriving economy, and protects privacy, civil rights, and civil liberties.

DHS Operations Integration

As a multi-mission agency, DHS covers diverse functions such as civil defense, emergency response, customs, border control, law enforcement, and immigration. Since its creation in 2002, DHS has strived to improve efficiency by eliminating duplication of effort in addressing common threats and hazards. DHS components have similar responsibilities and challenges, but often operate independently and do not unify their efforts, cooperate, or share information. Additionally, DHS headquarters does not always enforce its authority and ensure compliance with its guidance, which limits information sharing, coordination of assets, and integration of systems and processes. In April 2014, the Secretary



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

reaffirmed the need for increased departmental cohesiveness and leadership and initiated a strategy to unify the Department through the Unity of Effort Initiative.

FY 2014 Observations

Our FY 2014 audits identified several programs with weak department-level oversight. These audits showed the Department did not adequately manage common programs resulting in potentially excessive costs, inaccurate inventories, and unreliable data. For example, DHS and U.S. Immigration and Customs Enforcement (ICE) did not have a department-wide policy for management and administration to help standardize workers' compensation programs and reduce costs. In our audit of DHS' preparedness for pandemics, we found DHS did not effectively manage its stockpile of pandemic equipment and antiviral medications. In addition, we identified inaccurate inventories of pandemic preparedness supplies at component offices. As a result, the Department has no assurance it has sufficient equipment and medical countermeasures to respond to a pandemic.

We also audited DHS' use of home-to-work transportation and concluded that DHS does not have reliable and accurate data to determine whether participation in the program is justified. Additionally, neither DHS nor the components have systems to adequately track and monitor home-to-work-related data or gather it in a central system. Finally, DHS does not adequately manage or have the enforcement authority over its components' fleet operations to ensure that its motor vehicle fleet composition is right-sized. We estimated that operating these underused vehicles in FY 2012 cost between \$35.3 million and \$48.6 million in funds that could have been put to better use. Two reports issued in 2013 identified weaknesses in DHS management and cross-component coordination for the use of radio communications. This led to cost inefficiencies and problems using the equipment.

In September 2014, the Government Accountability Office (GAO) issued a report on DHS' coordination of vulnerability assessments, or assessments that can identify factors that render an asset or facility susceptible to threats and hazards. DHS has not issued guidance to the DHS offices or components involved in these assessments to ensure that the areas that DHS deems most important are captured in their assessment tools and methods. As a result, DHS was not positioned to integrate assessments to determine priorities between and across critical infrastructure sectors.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Management Progress and Next Steps

In May 2014, the GAO reported that DHS has made important progress in implementing, transforming, strengthening, and integrating its management functions. According to GAO, the Secretary, Deputy Secretary, the Under Secretary for Management, and other senior officials continued to demonstrate commitment and top leadership support for addressing the Department's management challenges.

To achieve cultural change, DHS must set the tone at the top, drive components to change, and empower its employees. DHS senior leadership has already set the tone for continued culture change, most recently in the Secretary's April 2014 Unity of Effort Initiative. Establishing cross-training opportunities and rotational or developmental assignments at multiple organizational levels could help DHS achieve a unified culture. These "cross-boundary partnerships" would increase the employees' awareness of comparable challenges among components and enhance their understanding of similarities and differences in programs and operations. The partnerships also allow them to build networks and expand coordination, enhance the sense of a single mission, help spread and apply best practices, and improve information sharing.

Acquisition Management

With the third largest acquisition budget in the Federal Government, DHS acquires more than \$18 billion worth of goods and services annually. Components did not always follow departmental acquisition guidance, which led to acquisition cost overruns, missed schedules, and lackluster acquisition performance. All of these have an effect on budget, security, and efficient use of resources. Even though DHS has initiated efforts to improve its acquisition processes, DHS leadership continues to authorize and invest in major acquisition programs that lack the foundational documents and management controls necessary to manage risks and measure performance.

FY 2014 Observations

In FYs 2013 and 2014, OIG audited acquisition management oversight of cost, schedule, and performance, compliance with the Department's acquisition framework, and coordination among components. The Department's programs continue to have problems with schedule delays,



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

cost overruns, and delivering promised capabilities. Additionally, lack of coordination among components can lead to program redundancy, inefficient use of resources, and security risks to programs. For example, DHS' Office of Program Accountability and Risk Management (PARM), which is responsible for overseeing departmental and component acquisition programs, was unable to schedule regular meetings of the Acquisition Review Board (ARB). This affects the Department's ability to provide consistent and effective oversight of billions of dollars of acquisitions.

In May 2013, we recommended that PARM apply all Acquisition Life Cycle Framework requirements from Management Directive 102-01 to the U.S. Customs and Border Protection's (CBP) Strategic Air and Marine Plan programs or projects. However, as of the end of FY 2014, the ARB had not met to implement the recommendation.

CBP did not effectively oversee and manage the fourth phase of the Advanced Training Center acquisition. Key acquisition documents supporting the \$55.7 million Interagency Agreement between CBP and the U.S. Army Corps of Engineers were either missing or incomplete. Specifically, CBP did not develop, review, or approve a required Independent Government Cost Estimate and Acquisition Plan prior to entering into the Interagency Agreement. CBP also approved millions of dollars' worth of contract modifications to the Interagency Agreement without first ensuring the need and reasonableness of the modifications. As a result, CBP could not adequately justify millions of dollars worth of labor and construction funding.

Management Progress and Next Steps

DHS has taken steps to improve acquisition oversight processes and controls by instituting the Acquisition Life Cycle Framework to provide acquisition management, support, review, and approval. PARM, created in 2011, has improved decision making in the last 3 years and provided insight on the health of the 112 programs on the Major Acquisition Oversight list. According to DHS, PARM is working with components to schedule ARB meetings and in FY 2014, the Department averaged one ARB meeting per month.

DHS needs to continue to improve and regularly assess the acquisition oversight and management of major programs. Efficient and effective acquisition management that complies with Federal regulations, policies, and procedures is critical to preventing waste and abuse and to ensuring



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

that goods and services are procured in a timely manner and at a reasonable cost.

Financial Management

The Federal Government must be an effective steward of taxpayer dollars. Sound financial practices and related management operations, financial information technology (IT) systems, and effective internal controls are essential to providing reliable, timely financial information to support management decision making needed 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.

FY 2014 Observations

In FY 2014, DHS obtained an unmodified (clean) opinion on all financial statements. In achieving this opinion, the Department continued to build on last year's success; however, as happened last year, it required considerable manual effort to overcome deficiencies in internal control and a lack of financial IT systems functionality.

In FY 2013, the independent auditors identified four material weaknesses, which persisted into FY 2014 — weaknesses in financial reporting; IT controls and financial systems functionality; property, plant, and equipment (PP&E); and budgetary accounting. The Department received an adverse opinion on internal control over financial reporting because of the existence of 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.

As in FY 2013, several components [United States Coast Guard (Coast Guard), ICE, Management Directorate (MGMT), National Protection and Programs Directorate (NPPD), and United States Secret Service (Secret Service)] contributed to a material weakness in financial reporting. Although MGMT and NPPD have assumed more responsibilities for financial management functions, they did not fully design internal controls. In addition, MGMT did not fully establish a financial



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

management infrastructure. The Secret Service had several controls that were not operating effectively. The internal control weaknesses that existed at the Office of Financial Management in the prior year were corrected in FY 2014.

During FY 2014, DHS components made progress in remediating IT findings reported in FY 2013. Although the auditors closed about 35 percent of prior year IT findings, in FY 2014, they identified 53 new findings at several DHS components. CBP, the Federal Emergency Management Agency (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. 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 2014. DHS' PP&E consists of aircraft, vessels, vehicles, land, structures, facilities, software, and other equipment, and the Transportation Security Administration's (TSA) passenger and baggage screening equipment. The Coast Guard maintains about 50 percent of DHS' PP&E. In FY 2013, the Coast Guard completed several phases of a multi-year remediation plan, addressing process and control deficiencies related to its PP&E assets, totaling about \$10.6 billion. However, the Coast Guard did not complete some remediation efforts scheduled for FY 2014 and currently has ongoing remediation activities planned for FY 2015. The auditors also noted that CBP continued to enhance controls and perform remediation to address deficiencies in the timely recording of capitalized costs and in the classification of PP&E.

The auditors identified a material weakness in budgetary accounting again in FY 2014. Although the Coast Guard, FEMA, ICE, MGMT, and NPPD continued to improve their policies and procedures for budgetary accounting processes, some control deficiencies reported in FY 2013 remained and new deficiencies were identified.

Management Progress and Next Steps

During FY 2014, DHS 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. In FY 2015 and beyond, DHS



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

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.

According to the Department, it has launched the Financial Systems Modernization initiative to expand business intelligence capabilities and modernize financial systems. DHS 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, reduce system sustainment costs, and further the Department's efforts to standardize business processes and data structures where possible.

IT Management and Privacy Issues

In managing IT processes and procedures, DHS, its components, and contractors continue to be challenged to develop integrated, cost-effective, and secure systems management policies; and protect personally identifiable information (PII). For example, in June 2014, a DHS contractor notified the Department of a breach that may have exposed the background check records of about 25,000 DHS employees. OIG will continue to evaluate the Department's progress in establishing and implementing a cost-effective, secure, and compatible IT infrastructure. This includes evaluations and reviews of the Department's data center consolidation and implementation of a standard IT platform, evaluation of component agency privacy programs and compliance, components' IT systems management, and DHS' efforts to protect PII.

FY 2014 Observations

IT plays a critical role in enabling U.S. Citizenship and Immigration Services (USCIS) to accomplish its mission. The USCIS Office of Information Technology (OIT) did not fully coordinate and communicate across OIT divisions, which hindered USCIS' ability to support mission needs and use allocated resources effectively. USCIS also faced significant challenges coordinating software licenses. Rather than OIT managing licenses and maintenance agreements centrally, each OIT division managed its own. In some cases, USCIS contractors installed more licenses than were available, which required USCIS management resolution. In addition, USCIS' complex IT systems, some made up of more than 29 commercial software products, impeded the component's work throughput. Time studies at USCIS service centers showed that



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

adjudicating applications and petitions for immigration benefits and services using paper-based processes was faster than adjudicating using the complex computer system.

DHS also did not ensure it had uniform procedures to implement privacy policies and controls to integrate privacy protections for each process, program, and information system that affects sensitive PII and protected information. DHS did not take appropriate steps to identify and mitigate physical risks to the security and confidentiality of records. For example, we observed instances in which passwords, sensitive IT information (such as server names or IP addresses), unsecured or unlocked credit cards and laptops, and printed materials marked “For Official Use Only” or containing sensitive PII could be accessed by individuals without a “need to know.”

NPPD continued to face challenges sharing and integrating cyber threat information among five Federal cyber operations centers and collaborating with them to respond to cybersecurity incidents. The cyber operations centers did not have a common incident management system to track, update, share, and coordinate cyber information. NPPD and the cyber operations centers also did not have a standardized set of categories for reporting cybersecurity incidents. Without these, NPPD and the centers continued to be challenged in sharing cyber incident information and coordinating an effective response.

Management Progress and Next Steps

OIT has made progress in addressing USCIS’ IT management issues. The Chief Information Officer has prioritized license maintenance renewals, and OIT has established a working group to manage all software and licensing agreements. OIT also began implementing a licensing and maintenance management process and created a position description for an individual to manage software acquisition, compliance with vendor contracts, maintenance renewals, and life cycle planning and costing. OIT is working to train its program office staff to ensure they use systems to their full extent. Further work needs to be done to address senior level staffing vacancies and improve coordination across OIT divisions.

DHS is also addressing the privacy risk of activities that involve PII. Specifically, the Enhanced Cybersecurity Services Program completed and published a privacy impact assessment.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

NPPD is also taking steps to better coordinate and share vital cyber threat information with the five Federal cyber operations centers. For example, NPPD has established partnerships with the other centers to coordinate an effective response on cyber incidents. In addition, NPPD has increased interagency collaboration and communication through liaisons and regular meetings. However, DHS must procure cyber tools and technologies and develop a standard set of cyber incident reporting categories to use with its operations center partners. DHS must also ensure its contractors have adequate controls in place to protect PII.

Transportation Security

The TSA's mission is to protect the Nation's transportation systems and ensure the freedom of movement for people and commerce. For aviation security, TSA conducts screening operations at federalized airports. TSA uses various security technologies and programs to screen passengers and their baggage for weapons, explosives, and other prohibited items, as well as to prevent unauthorized access by individuals to secured airport areas. TSA needs to continue to improve the security of the national transportation systems by ensuring it minimizes human- and technology-based errors and vulnerabilities, uses resources efficiently, and assesses program effectiveness.

FY 2014 Observations

Our recent audits of transportation security showed that TSA needs to improve the performance of its baggage and passenger screening workforce, use its resources strategically and efficiently, and assess its program performance.

Through covert testing at domestic airports, we sought to determine whether transportation security officers were following policies and procedures to prevent threat items from being placed onto commercial aircraft and to determine the effectiveness of checked baggage screening technology. Specific results are classified, but we identified human- and technology-based failures that led to vulnerabilities in screening. In addition, we identified weaknesses in assessing the functionality of checked baggage screening equipment.

In our audit of TSA's deployment and use of advanced imaging technology (AIT), we determined TSA did not have a comprehensive



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

deployment strategy to ensure all AIT units were deployed effectively and used fully for optimal screening of passengers.

We determined that TSA's Office of Inspection did not use its staff and resources efficiently to conduct cost-effective inspections, internal reviews, and covert testing. Additionally, the office did not properly plan its work and resource needs, did not have sufficient quality controls over its work, and could not always ensure other TSA components took action on its recommendations to improve TSA's operations. As a result, the Office of Inspection may not have fully accomplished its mission to identify and address transportation security vulnerabilities.

TSA's Screening of Passengers by Observation Techniques (SPOT) program continued to be a challenge. In FY 2013, we reported that TSA did not implement a strategic plan or assess program effectiveness. According to an FY 2014 GAO report, TSA had limited information to evaluate SPOT's effectiveness. Until TSA can provide scientifically validated evidence that behavioral indicators can be used to identify passengers who may pose a threat to aviation security, the component risks funding activities that may not be effective.

Management Progress and Next Steps

TSA has taken actions to comply with our recommendations. For example, the component began to develop screening equipment deployment strategies that address short- and long-term goals. TSA's Office of Inspection began taking steps to improve use of staffing and resources and to improve the quality and effectiveness of its work. TSA needs to continue planning strategic deployment of new screening technologies. Without comprehensive, strategic deployment plans and processes for approving changes to plans, TSA decision makers do not have a systematic approach to maximizing technology advances for reducing current and evolving threats. Additionally, TSA needs to continue testing its technology and screening personnel to ensure they are prepared to prevent weapons, explosives, and other prohibited items from being loaded onto the Nation's transportation systems.

Border Security and Immigration Enforcement

CBP, ICE, the Coast Guard, and USCIS must work together to detect, deter, and interdict illegal entry of people and contraband into the United States, as well as apprehend, process, and determine the status of



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

immigrants. Smugglers and drug traffickers threaten border security by targeting those crossing the border legally and by trying to corrupt CBP officers and border patrol agents. Protecting our borders and addressing both illegal and legal immigrants requires communication and collaboration among components, between component headquarters and their field offices, and between components and DHS headquarters. The components also need to implement policies consistently, especially among their field offices, and make certain operations are properly documented so DHS headquarters has timely, reliable data and information. The Department must ensure that it provides consistent guidance to components and enforces compliance.

FY 2014 Observations

CBP needs effective internal controls over its programs and should share program data with other DHS components and Federal agencies to identify illegal cross-border activities and trends. CBP's Secure Electronic Network for Travelers Rapid Inspection (SENTRI) program is designed to accelerate inspection of low-risk travelers at southern ports of entry. However, some participants in the program abused their privileges and transported illicit goods across the border. Smugglers and drug traffickers also tried to use participants as conduits for illegal cross-border activities.

Insufficient communication among components and between components and the Department can be detrimental to program effectiveness. In February and March 2013, media sources reported that ICE released hundreds of immigrant detainees, including some with criminal convictions. Prior to releasing the detainees, ICE leadership did not communicate effectively with its office of Enforcement and Removal Operations (ERO). ICE also did not inform DHS leadership or the Executive Office of the President about a budget shortfall, and it did not notify the DHS Secretary about its plans to release aliens.

Under its worksite enforcement strategy, ICE seeks to deter employers who knowingly hire illegal workers and identify and penalize those who do so. In carrying out this strategy, ICE's Homeland Security Investigations (HSI) headquarters did not adequately oversee some of its field offices to ensure they were consistent in issuing warnings and fines. HSI also did not analyze the effect of these differences in implementation or sufficiently determine whether implementation improved compliance.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

In addition, field offices did not always maintain adequate, up-to-date documentation.

The Employment-Based Fifth Preference (EB-5) program was designed to stimulate the U.S. economy through job creation and capital investment by foreign investors. USCIS did not effectively administer and manage its EB-5 regional center program. USCIS had difficulty ensuring program integrity. Not all EB-5 regional centers met program eligibility requirements. USCIS officials also interpreted Federal regulations and policies differently. USCIS did not always document decisions and responses to inquiries about the program. Thus, USCIS was limited in its ability to prevent fraud or national security threats and could not demonstrate the program improved the economy and created jobs.

During the last year, CBP was challenged by an increasing number of unaccompanied children crossing the southwest border from Central America. In July 2014, OIG began site visits of CBP's short-term holding facilities for these children to assess the treatment of children in custody. We reported that not all facilities posted copies of policies for unaccompanied children or maintained inventories of their property. OIG, ICE, and CBP also began investigating allegations of criminal behavior, as well as violations of civil rights, liberties, laws, regulations, and policies.

Management Progress and Next Steps

CBP, ICE, and USCIS have taken steps to implement our report recommendations. Since our initial review of the SENTRI program in 2004, CBP has enhanced its internal controls and begun addressing issues related to officer integrity. As a result of our more recent report, CBP began implementing our recommendations to mitigate the risk of employee corruption and improve information sharing. To improve its processes for retention and release of detainees, ICE plans to provide information on funding resources to ERO and pursue long-term budget authority for full funding for detention of aliens. In carrying out its worksite enforcement strategy, ICE started to develop a process to evaluate the effectiveness of its inspections of employers. For the EB-5 program, USCIS has taken action to process applications and petitions consistently, increase coordination with other Federal agencies, evaluate the economic impact of the program, and enhance quality assurance and program integrity.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Although DHS and its components concurred with virtually all of our recommendations and have taken steps to improve, they need to continue their efforts to enhance communication and coordination, better track and maintain data, and implement and enforce consistent policies and procedures.

Grants Management

Grants have a significant role in the mission of the Department and FEMA to help save lives and protect property. DHS grants are used to fund disaster assistance, disaster preparedness, and infrastructure security; they also fund scientific research intended to improve national security. In the most recent budget submitted to Congress, the President estimated that during FY 2014, FEMA would spend more than \$14 billion in grants. Historically, the Department has faced significant challenges in ensuring that grantees spend these funds according to Federal regulations. The challenges result from, among other causes, increased grant funding, ambiguous grant objectives, and passive grant management and lack of oversight by FEMA and the states.

FEMA's increased challenges in managing disaster assistance are due in part to a rise in the number of declared disasters. In the 1980s, the President declared an average of only about 24 major disasters per year. In the past 10 years, the number has risen to an average of 65 major disasters annually. According to FEMA's public website, from calendar years 2004 to 2013, the President approved 654 requests from governors to declare national disasters. These declarations resulted in FEMA obligating nearly \$99 billion—or about \$10 billion annually—from the Disaster Relief Fund.

FY 2014 Observations

FEMA continues to experience challenges managing the immense and risky disaster assistance program. Currently, every state and most of the U.S. possessions have open disasters that include more than 100,000 grant applicants spending more than \$50 billion on more than 600,000 disaster assistance projects. Earlier this year, we issued a report summarizing the results of our disaster assistance audits for the last 5 years. In that report, it was noted that, of the \$5.9 billion that we audited, disaster assistance recipients did not properly spend \$1.36 billion, or an average of 23 percent, of the disaster assistance grants.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

The Department also provides Homeland Security Grant Program funds to state, territory, local, and tribal governments to enhance their ability to prepare for, prevent, protect, respond to, and recover from terrorist attacks, major disasters, and other emergencies. The program includes several interrelated Federal grant programs that fund a range of preparedness activities including planning, organization, equipment purchases, training, and exercises, as well as management and administration. Since 2007, we have audited states and urban areas to determine whether they have implemented their grants efficiently and effectively, achieved program objectives, and spent funds according to grant requirements.

In these Homeland Security Grant Program audits, we determined that in most instances the states complied with applicable laws and regulations in distributing and spending their preparedness grant awards. However, we noted several challenges in developing state homeland security strategies, obligating grant funds in a timely manner, reimbursing expenses, and monitoring subgrantee grant management.

Management Progress and Next Steps

Since Hurricane Katrina in 2005, FEMA has significantly improved its ability to lead the Nation's response and recovery efforts. However, the component needs to do more to mitigate the inherent risks of its disaster assistance grants. In the past, FEMA and the states provided more passive grant oversight; hoping grant recipients would spend the grant funds correctly. In response to OIG reports, FEMA recently initiated a number of proactive actions to address past shortfalls. Although FEMA still faces significant management challenges, OIG is committed to helping FEMA officials address the causes of noncompliance. Other DHS components that award grants should also continue to identify instances of noncompliance and close the gaps inhibiting effective grant management.

Employee Accountability and Integrity

The Department has nearly 250,000 Federal employees with another 250,000 contract employees who are responsible for protecting and securing the Nation. The vast majority of these employees are honest, dedicated public servants, yet those who are not, can do incalculable damage to our national security.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

FY 2014 Observations

In FY 2014, we have received approximately 16,281 complaints and opened more than 500 investigations. In that same period, approximately 100 cases were accepted for prosecution. We have achieved 112 convictions and effected 36 personnel actions.

Our investigations cover a large scope of unlawful activities and misconduct in which DHS employees engage or that otherwise affect the Department's programs. Investigations related to employee accountability and integrity occur when Department employees, who have inside information concerning the organization's security procedures, contracting practices, and property management, use that information for personal gain. The following sample of our casework demonstrates the breadth of our FY 2013 and FY 2014 casework across many DHS components.

Two investigations illustrate the nature of the threat along our southwest border. As acknowledged in their plea agreements, a border patrol agent and a former state prison guard formed a "criminal partnership" to earn money by helping traffickers smuggle drugs and aliens into the United States. As part of this multi-year partnership, the border patrol agent accepted bribes from the former state prison guard in exchange for providing him with sensitive information, including sensor maps, combinations to gates located near the Mexican border, computer records of prior drug seizures, and the location of border patrol units. The agent and former prison guard were sentenced to prison for 15 years and 9 years, respectively. In another case, while patrolling the border with Mexico, a border patrol agent driving a marked government vehicle helped three individuals on the Mexican side of the border smuggle bales of marijuana weighing 147 pounds into the United States. The agent pled guilty to possession of a firearm in furtherance of a drug trafficking offense and was subsequently sentenced to 60 months in prison.

We investigated a TSA supervisory transportation security officer in the U.S. Virgin Islands who was actively assisting a drug smuggling organization to bypass security at an airport. He was sentenced to 87 months imprisonment and 24 months of supervised release.

In another case, a senior Federal Protective Service acquisitions official was sentenced to 16 months imprisonment for conspiracy to receive bribes by a government official. He conspired with two others to unlawfully steer Federal security guard contracts. One co-conspirator



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

was sentenced to 72 months imprisonment and forfeiture of more than \$6 million; the second was sentenced to 48 months imprisonment, forfeiture of more than \$1.2 million and a fine of \$1 million.

An investigation of a Coast Guard civilian employee revealed that he used his position to steer contracts to a specific company that specialized in shipping services in return for more than \$200,000 in kickbacks. Ultimately, these questionable shipments resulted in a fraud loss to the Government of about \$1 million. The Coast Guard employee pled guilty and was sentenced to 87 months incarceration and 36 months of supervised release. The company owner pleaded guilty and was sentenced to 63 months incarceration and 36 months of supervised release and ordered to pay a \$15,000 fine and restitution.

We also investigated the owner of a supply company who falsely certified that the aircraft parts he was providing DHS were within Federal Aviation Administration guidelines. He was sentenced to 30 months incarceration and 36 months of supervised release.

Management Progress and Next Steps

The Department continues to recognize the potential waste, duplication, and opportunities for fraud that exists in a non-enterprise approach to procurement. DHS has developed and delivered a comprehensive acquisition training program for DHS Employees. As of FY 2014, DHS has invited DHS OIG to conduct presentations on acquisition corruption and fraud awareness during the training.

Infrastructure Protection, Cybersecurity, and Insider Threat

Cybersecurity risks, especially intrusions into critical infrastructure areas, pose serious economic and national security challenges for our Nation. The United States' open and technologically complex society includes a wide array of critical infrastructure and key resources that are potential terrorist targets.¹ Cybersecurity involves implementing

¹ 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. Key resources are publicly or privately controlled assets essential to minimal operation of the economy and Government.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

protective measures to secure cyberspace and its associated infrastructure, such as protecting computers and networks from accidental or malicious harm by preventing, detecting, and responding to risks and attacks. It also includes restoring information systems and data within them to ensure system confidentiality, integrity, and availability. To ensure their continuity and viability, DHS needs to frequently assess the reliability of critical infrastructure, as well as its vulnerability to threats—including insider threats. DHS also needs to share cyber threat information with its stakeholders. Because the technology and nature of threats change rapidly, so must the protective measures and responses.

NPPD leads DHS' effort to protect and enhance the resiliency of physical and cyber infrastructure. This critical infrastructure provides essential services to security, economic welfare, public health, and safety. NPPD provides information, tools, and analyses to help public and private sector infrastructure owners and operators reduce risks through informed decision making. NPPD's Office of Cybersecurity and Communications Enhanced Cybersecurity Security (ECS) Program shares sensitive and classified government-vetted cyber threat information with qualified Commercial Service Providers. In turn, the Commercial Service Providers use the cyber threat information to protect their customers, who are validated critical infrastructure entities from all 16 sectors. However, DHS continues to face challenges sharing cyber incident information with Federal cyber operations centers and coordinating effective responses.

FY 2014 Observations

The Department is responsible for conducting comprehensive vulnerability assessments of critical infrastructure; integrating relevant information, analyses, and assessments from within DHS and from critical infrastructure partners; and using the information collected to identify priorities for protective and support measures. A recent GAO audit reported that DHS offices and components have not consistently captured and maintained data on vulnerability assessment activities in a way that allows DHS to identify potential duplication or overlap in coverage among vulnerability assessment activities they have conducted or required. As a result, DHS is not positioned to track its activities to determine whether its assessment efforts are potentially duplicative or leave gaps among the critical infrastructure assessed. DHS must ensure effective risk management across the spectrum of assets and systems, as called for by the National Infrastructure Protection Plan.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

The ECS program has been slow to expand because of limited outreach and resources. As of March 2014, entities from only 3 of the 16 critical infrastructure sectors (defense industrial base, energy, and communication services) were receiving ECS program services. Furthermore, only two operational commercial service providers were enrolled in the program. Although the Office of Cybersecurity and Communications was promoting the ECS program, it was not communicating directly with critical infrastructure entities about the benefits of participating. In addition, NPPD relied on manual reviews and analyses to share cyber threat information, which led to inconsistent quality in cyber threat indicators.

DHS faced challenges in sharing cyber information among Federal cyber operations centers. In addition, insufficient staffing levels hindered continuous coverage in all mission areas in the National Cybersecurity and Communications Integration Center and the Office of Intelligence and Analysis. Staff members also needed additional technical training to improve incident response. Finally, NPPD's Continuity of Operations Plan needed to be updated, finalized, and integrated with other continuity of operations plans.

DHS and the Domestic Nuclear Detection Office (DNDO) both took steps to address and mitigate the risk of insider threats to the cybersecurity of DNDO's IT systems and sensitive information. In September 2013, for example, DHS began a vulnerability assessment of DNDO's assets, which included identifying insider threats and vulnerabilities. DNDO also participated in the Insider Threat Task Force, but did not define roles and responsibilities for addressing insider threats to unclassified networks and systems. DNDO also could not document the effectiveness of controls that detect and respond to unauthorized data transfers from its unclassified IT assets via DHS email services. DNDO had not installed critical security patches to its IT assets.

Management Progress and Next Steps

NPPD has made progress in expanding the ECS program. As of May 2014, 40 critical infrastructure entities were participating, and 22 companies had signed memorandums of agreement to join. NPPD also established program procedures and guidance, expanded the program to sector-specific agencies and government-furnished information providers, and developed reporting and metrics for program monitoring. NPPD concurred with all three of our report recommendations and has taken steps to implement them.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

NPPD is taking steps to better coordinate and share vital cyber threat information with the five Federal cyber operations centers. NPPD also took steps to address our recommendations to increase staffing, enhance training, and update its Continuity of Operations Plan.

Once the DHS Office of the Chief Information Officer issues an insider threat policy, DNDO should strengthen processes and controls for its IT infrastructure by implementing updated insider threat procedures. DNDO also needs to document the effectiveness of controls or processes to detect and respond to unauthorized data exfiltration from its unclassified IT assets. DNDO can strengthen processes and controls for its own technology infrastructure by disabling portable media ports on controlled IT assets where there is no legitimate business need. DNDO should also ensure that critical security patches are applied to these assets and periodically assess the security of controlled sites to identify unauthorized wireless devices or connections to DHS networks. DNDO concurred with all our recommendations and began taking steps to implement them.



Appendix A

Relevant Reports

DHS OIG reports can be found under the “Reports” tab at <http://www.oig.dhs.gov/>

Background

- DHS, *DHS Budget-in-Brief*, Fiscal Year 2015.
<http://www.dhs.gov/sites/default/files/publications/FY15BIB.pdf>
- DHS, *The 2014 Quadrennial Homeland Security Review*, June 2014.
<http://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf>

DHS Operations Integration Challenges

- DHS-OIG, *DHS Has Not Effectively Managed Pandemic Personal Protective Equipment and Antiviral Medical Countermeasures* (OIG-14-129, August 2014).
http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-129_Aug14.pdf
- DHS-OIG, *Does Not Adequately Manage or Have Enforcement Authority Over Its Components’ Vehicle Fleet Operations* (OIG-14-126, August 2014).
http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-126_Aug14.pdf
- DHS-OIG, *U.S. Immigration and Customs Enforcement’s Management of Federal Employees’ Compensation Act Program* (OIG-14-105, July 2014).
http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-105_Jul14.pdf
- DHS-OIG, *DHS Conference Spending* (OIG-14-82, April 2014).
http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-82_Apr14.pdf
- DHS-OIG, *Fiscal Year 2013 Risk Assessment of DHS Charge Card Abuse Prevention Program* (OIG-14-29, January 2014).
http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-29_Jan14.pdf
- DHS-OIG, *DHS Home-to-Work Transportation* (OIG-14-21, December 2013).
http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-21_Dec13.pdf
- DHS-OIG, *DHS Needs to Manage Its Radio Communication Program Better* (OIG-13-113, August 2013).
http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-113_Aug13.pdf
- DHS-OIG, *DHS’ Oversight of Interoperable Communications* (OIG-13-06, November 2012).
http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-06_Nov12.pdf



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

- GAO, *Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts*. (GAO-14-507, September 2014).
<http://www.gao.gov/assets/670/665788.pdf>

Acquisition Management Challenges

- DHS-OIG, *U.S. Customs and Border Protection's Advanced Training Center Acquisition* (OIG-14-47, February 2014).
http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-47_Feb14.pdf
- DHS-OIG, *Transportation Security Administration's Deployment and Use of Advanced Imaging Technology* (OIG-13-120, March 2014).
http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-120_Mar14.pdf
- DHS-OIG, *DHS' H-60 Helicopter Program* (OIG-13-89, May 2013).
http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-89_May13.pdf

Financial Management Challenges

- DHS-OIG, *Independent Auditor's Report on DHS' FY 2013 Financial Statements and Internal Control over Financial Reporting* (OIG-14-18, December 2013).
http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-18_Dec13.pdf
- DHS-OIG, *Independent Auditor's Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting* (OIG-15-10, November 2014).
http://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-10_Nov14.pdf

IT Management and Privacy Challenges

- 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
- DHS-OIG, *U.S. Citizenship and Immigration Services Information Technology Management Progress and Challenges* (OIG-14-112, July 2014).
http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-112_Jul14.pdf
- DHS-OIG, *Information Technology Management Letter for the FY 2013 Department of Homeland Security's Financial Statement Audit – Office of Financial Management and Office of Chief Information Officer* (OIG-14-108, 06/24/14).
http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-108_Jun14.pdf



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

- DHS-OIG, *DHS' Efforts to Coordinate the Activities of Federal Cyber Operations Centers* (OIG-14-02, October 2013).
http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-02_Oct13.pdf

Transportation Security Challenges

- DHS-OIG, (U) *Vulnerabilities Exist in TSA's Checked Baggage Screening Operations* (OIG-14-142, September 2014).
http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_SLP_14-142_Sep14.pdf
- DHS-OIG, *Transportation Security Administration Office of Inspection's Efforts to Enhance Transportation Security* (OIG-13-123, September 2013).
http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-123_Sep13.pdf
- DHS-OIG, *Transportation Security Administration's Deployment and Use of Advance Imaging Technology* (OIG-13-120, March 2014).
http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-120_Mar14.pdf
- DHS-OIG, *Transportation Security Administration's Screening of Passengers by Observation Techniques* (REDACTED) (OIG-13-91, May 2013).
http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-91_May13.pdf

Border Security and Immigration Enforcement Challenges

- DHS-OIG, *ICE's Release of Immigration Detainees (Revised)* (OIG-14-116, August 2014).
http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-116_Aug14.pdf
- Memo to DHS Secretary Johnson from Inspector General Roth, July 30, 2014, Oversight of Unaccompanied Alien Children
- Intelligence Community Joint Report, *Unclassified Summary of Information Handling and Sharing Prior to the April 15, 2013 BOSTON MARATHON BOMBINGS*, (April 2014)
http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_Bos_Marathon_Bom_Rev_Apr14.pdf
- DHS-OIG, *U.S. Immigration and Customs Enforcement's Worksite Enforcement Administrative Inspection Process* (OIG-14-33, February 2014).
http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-33_Feb14.pdf



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- DHS-OIG, (U) *Ensuring the Integrity of CBP's Secure Electronic Network for Travelers Rapid Inspection Program* (OIG-14-32, February 2014).
http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-32_Feb14.pdf
- DHS-OIG, *Adequacy of USSS Efforts to Identify, Mitigate, and Address Instances of Misconduct and Inappropriate Behavior* (Redacted) (OIG-14-20, December 2013).
http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-20_Dec13.pdf
- DHS-OIG, *U.S. Citizenship and Immigration Services' Employment-Based Fifth Preference (EB-5) Regional Center Program* (OIG-14-19, December 2013).
http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-19_Dec13.pdf

Grants Management Challenges

- DHS-OIG, *FEMA's Progress in Clarifying its "50 Percent Rule" for the Public Assistance Grant Program* (OIG-14-123-D, August 2014).
http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-123-D_Jul14.pdf
- DHS-OIG, *New York City's Department of Transportation Needs Assistance to Ensure Compliance with Federal Regulations* (OIG-14-120-D, July 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-120-D_Jul14.pdf
- DHS-OIG, *New York City's Department of Design and Construction Needs Assistance To Ensure Compliance with Federal Regulation* (OIG-14-115-D, July 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-115-D_Jul14.pdf
- DHS-OIG, *FEMA Should Recover \$3.9 Million of Public Assistance Grant Funds Awarded to Jefferson County, Alabama, as a Result of Severe Storms in April 2011* (OIG-14-114-D, July 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-114-D_Jul14.pdf
- DHS-OIG, *FEMA's Initial Response to the Colorado Flood* (OIG-14-111-D, July 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-111-D_Jul14.pdf
- DHS-OIG, *Mitigation Planning Shortfalls Precluded FEMA Hazard Mitigation Grants to Fund Residential Safe Room Construction During the Disaster Recovery Phase* (OIG-14-110-D, June 2014).



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-110-D_Jun14.pdf

- DHS-OIG, *FEMA Should Recover \$1.3 Million of Public Assistance Grant Funds Awarded to Desire Street Ministries, New Orleans, Louisiana, for Hurricane Katrina* (OIG-14-107-D, June 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-107-D_Jun14.pdf
- DHS-OIG, *FEMA Should Recover \$764,968 of Public Assistance Program Grant Funds Awarded to the University of Hawaii, Honolulu, Hawaii* (OIG-14-104-D, June 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-104-D_Jun14.pdf
- DHS-OIG, *Capping Report: FY 2013 FEMA Public Assistance and Hazard Mitigation Grant and Subgrant Audits* (OIG-14-102-D, June 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-104-D_Jun14.pdf
- DHS-OIG, *FEMA's Slab Removal Waiver in Oklahoma 4117-DR-OK* (OIG-14-100-D, June 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-100-D_Jun14.pdf
- DHS-OIG, *FEMA Should Recover \$8.0 Million of \$26.6 Million in Public Assistance Grant Funds Awarded to St. Stanislaus College Preparatory in Mississippi – Hurricane Katrina* (OIG-14-95-D, May 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-104-D_Jun14.pdf
- DHS-OIG, *FEMA Could Realize Millions in Savings by Strengthening Policies and Internal Controls Over Grant Funding for Permanently Relocated Damaged Facilities* (OIG-14-91-D, May 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-91-D_May14.pdf
- DHS-OIG, *FEMA Should Review the Eligibility of \$523,007 of \$5.4 Million in Public Assistance Grant Funds Awarded to the Borough of Belmar, New Jersey, for Hurricane Sandy Debris Removal Activities* (OIG-14-72-D, April 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-72-D_Apr14.pdf
- DHS-OIG, *FEMA Should Recover \$1.7 Million of Public Assistance Grant Funds Awarded to the City of Waveland, Mississippi – Hurricane Katrina* (OIG-14-63-D, April 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-63-D_Apr14.pdf



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

- DHS-OIG, *The Village of Saltaire, New York, Generally Managed FEMA's Public Assistance Grant Funds Effectively* (OIG-14-58-D, March 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-58-D_Mar14.pdf
- DHS-OIG, *FEMA Should Review the Eligibility of \$689,138 of \$5.57 Million in Public Assistance Grant Funds Awarded to Little Egg Harbor Township, New Jersey, for Hurricane Sandy Debris Removal Activities* (OIG-14-57-D, March 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-57-D_Mar14.pdf
- DHS-OIG, *Santa Cruz Port District Generally Followed Regulations for Spending FEMA Public Assistance Funds* (OIG-14-56-D, March 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-56-D_Mar14.pdf
- DHS-OIG, *FEMA Should Recover \$3.7 Million in Unneeded Funds and Review the Eligibility of \$344,319 of \$5.84 Million in Public Assistance Grant Funds Awarded to the Borough of Beach Haven, New Jersey, for Hurricane Sandy Debris Removal Activities* (OIG-14-54-D, March 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-54-D_Mar14.pdf
- DHS-OIG, *FEMA Should Recover \$2.3 Million of Unsupported, Unused, and Ineligible Grant Funds Awarded to East Jefferson General Hospital, Metairie, Louisiana* (OIG-14-53-D, March 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-53-D_Mar14.pdf
- DHS-OIG, *FEMA's Initial Response to the Oklahoma Severe Storms and Tornadoes* (OIG-14-50-D, March 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-50-D_Mar14.pdf
- DHS-OIG, *FEMA Should Recover \$8.2 Million of the \$14.9 Million of Public Assistance Grant Funds Awarded to the Harrison County School District, Mississippi—Hurricane Katrina* (OIG-14-49-D, March 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-49-D_Mar14.pdf
- DHS-OIG, *FEMA's Dissemination of Procurement Advice Early in Disaster Response Periods* (OIG-14-46-D, February 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-46-D_Feb14.pdf
- DHS-OIG, *FEMA Should Recover \$5.3 Million of the \$52.1 Million of Public Assistance Grant Funds Awarded to the Bay St. Louis Waveland*



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

School District in Mississippi—Hurricane Katrina (OIG-14-44-D, February 2014).

http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-44-D_Feb14.pdf

- DHS-OIG, *The City of Raleigh, North Carolina, Properly Accounted for and Expended FEMA Public Assistance Grant Funds Awarded for April 2011 Disaster* (OIG-14-34-D, February 2014).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-34-D_Feb14.pdf
- DHS-OIG, *FEMA Should Recover \$10.9 Million of Improper Contracting Costs from Grant Funds Awarded to Columbus Regional Hospital, Columbus, Indiana* (OIG-14-12-D, December 2013).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-12-D_Dec13.pdf
- DHS-OIG, *FEMA Should Recover \$6.1 Million of Public Assistance Grant Funds Awarded to Orlando Utilities Commission under Hurricane Frances* (OIG-14-11-D, December 2013).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-11-D_Dec13.pdf
- DHS-OIG, *FEMA Should Recover \$48.9 Million for Inadequate Insurance Coverage for Holy Cross School, New Orleans, Louisiana* (OIG-14-10-D, November 2013).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-10-D_Nov13.pdf
- DHS-OIG, *Santa Cruz County, California, Generally Followed Regulations for Spending FEMA Public Assistance Funds* (OIG-14-03-D, October 2013).
http://www.oig.dhs.gov/assets/GrantReports/2014/OIG_14-03-D_Oct13.pdf

Employee Accountability and Integrity Challenges

- DHS-OIG, *Semi-Annual Report to Congress, 10/1/2013-3/31/2014*.
http://www.oig.dhs.gov/assets/SAR/OIG_SAR_Oct13_Mar14.pdf
- DHS-OIG, *Semi-Annual Report to Congress, 4/1/2014-9/30/2014*.
http://www.oig.dhs.gov/assets/SAR/OIG_SAR_Apr14_Sep14.pdf

Infrastructure Protection, Cybersecurity, and Insider Threat Challenges

- DHS-OIG, *Implementation Status of the Enhanced Cybersecurity Services Program* (OIG-14-119, July 2014).



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-119_Jul14.pdf
DHS-OIG, *Domestic Nuclear Detection Office Has Taken Steps to Address Insider Threat, but Challenges Remain* (OIG-14-113, July 2014).
 - http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-113_Jul14.pdf
DHS-OIG, *DHS's Efforts to Coordinate the Activities of Federal Cyber Operations Centers* (OIG-14-02, October 2013).
 - http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-02_Oct13.pdf
GAO, *Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts*. (GAO-14-507, September 2014).
- <http://www.gao.gov/assets/670/665788.pdf>



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B Management Comments to the Draft Report

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



**Homeland
Security**

November 10, 2014

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-15-9, "Major Management and
Performance Challenges Facing the Department of Homeland
Security" (Project No. 14-033-AUD-MGMT)

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) welcomes the Office of Inspector General's (OIG's) perspective on the most serious management and performance challenges facing the Department. DHS recognizes, as the OIG states, that "Some of the most persistent challenges arise from the effort to combine and coordinate diverse legacy agencies into a single, cohesive organization capable of fulfilling a broad, vital, and complex mission."

This, in part, is exactly why Secretary Jeh Johnson launched the DHS Unity of Effort Initiative earlier this year to build important linkages between the Department's planning, programming, budgeting, and execution processes, and ensure that DHS invests and operates in a cohesive, unified fashion, and makes decisions that are transparent and collaborative to drive strategic guidance to results. This initiative has already achieved many successes in strengthening DHS's existing business processes, developing new ones in areas of need, and re-orienting a number of headquarters functions.

It is important to note that DHS missions are complex and highly diverse, necessitating sustained management attention to succeed, while improving the effectiveness and efficiency of its many programs and operations. Also complicating matters are the resource constraints the Department faces, which have provided the impetus, as Secretary Johnson has previously said, "to build and mature our organization into one that is greater than the sum of its parts—one that operates with much greater unity of effort."



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

DHS remains committed to seeking improvements to how it operates collectively to more effectively and efficiently secure the homeland. A few selected successes and accomplishments relevant to the OIG's reported challenge areas are identified below:

Challenge #1: DHS Operations Integration

DHS has made considerable progress in establishing new processes—and strengthening existing ones—to improve its planning, programming, budgeting, and execution system. DHS headquarters and Operating Component senior leadership have reoriented their thinking based on the understanding that DHS must have better traceability between strategic objectives, budgeting, acquisition decisions, operational planning, and mission execution, to improve both Departmental cohesiveness and operational effectiveness. Through the “Unity of Effort” initiative, DHS is making changes intended to transparently incorporate DHS Components, through the establishment of Secretary- and Deputy Secretary-chaired leadership forums, into unified decision-making processes and, through the strengthening and reconciling of subordinate governance structures, the analytic efforts that inform decision-making. The overall goal is to better understand the broad and complex DHS mission space and empower DHS Components to effectively execute their operations.

For example, in April 2014, Secretary Johnson re-established the component-chaired Joint Requirements Council (JRC), which allows DHS to look at cross-component requirements and develop recommendations for investments, changes to training, organizational structure, laws, and operational processes. This new process is already enhancing operational effectiveness and better informing the Department's main investment pillars: (a) program and budget review and (b) the acquisition review process. The JRC has launch portfolio teams that are staffed by component operators and appropriate DHS headquarters personnel and organized by the five homeland security mission areas identified in the Quadrennial Homeland Security Review.

The JRC will help the Department better address joint requirements and close capability gaps for investments in areas such as: aviation commonality, information sharing, cybersecurity, information-based screening & vetting, and radio interoperability. To facilitate more efficient budget planning, the Office of the Chief Financial Officer is a principal member on the Council. Further, Secretary Johnson is providing formal guidance to ensure that operational planning is driven by strategic intent and include outcomes and quantified targets to better inform the joint requirements process and resource decisions.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Challenge #2: Acquisition Management

The Office of Program Accountability and Risk Management (PARM) provides the Department's central oversight of acquisition program management, which includes managing program governance, program support, and issuing acquisition program management policy. PARM has been working with Components to prepare for and schedule Acquisition Review Boards (ARBs) when programs are ready for an acquisition decision event. During FY 2014, 12 ARBs were held, resulting in the cancellation of one program and two others being paused.

In an effort to further strengthen oversight, the Under Secretary for Management, who also serves as the Department's Acquisition Decision Authority, chairs a monthly meeting with all ARB members, to receive and discuss information on high visibility major acquisition programs. In response to OIG's "DHS' H-60 Helicopter Programs" audit, PARM has provided regular updates on preparations for the Strategic Air and Marine Plan program's ARB. An Acquisition Decision Memorandum signed just last month directed program officials to prepare for an ARB within 30 days, and identified requirements and documentation needed. Other pre-ARB activities have included senior leadership meetings to clarify the importance of the ARB, review of additional procurement or transfer plans by the Chief Readiness Support Officer-chaired Aviation Governance Board and the JRC, and a detailed analysis of the Flight Hour Account (i.e., total cost to operate), all intended to help ensure adherence to departmental acquisition guidance, elimination of acquisition cost overruns and missed schedules, and to improve overall program performance.

Challenge #3: Financial Management

As the draft report acknowledges, DHS continues to build on last year's successful unmodified (clean) opinion by earning a second consecutive clean opinion on all financial statements. This achievement demonstrates DHS's sustained financial management progress due to the hard work of the men and women of this Department and the solid foundation of financial policies, processes and internal controls we built. DHS agrees with OIG that there are more areas for improvement and is working to achieve our goal of obtaining a clean opinion on internal control over financial reporting by FY 2016. We remain 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. These funds are dedicated to meet our core mission areas: prevent terrorism and enhance security; secure and manage our borders; enforce and administer our immigration laws; safeguard and secure cyberspace; strengthen



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

national preparedness and resilience; and mature and strengthen homeland security. The entire DHS financial management community has made great strides each year in our shared responsibility to deliver effective and efficient financial management services in support of our mission.

In FY 2014, U.S. Immigration and Customs Enforcement (ICE) and U.S. Citizenship and Immigration Services (USCIS) cleared their significant deficiency conditions in Information Technology (IT) and the Office of Financial Management cleared a significant deficiency condition in Financial Reporting. In FY 2013, the U.S. Coast Guard (USCG) made tremendous progress in their Property, Plant & Equipment line item and continued to reduce severity in FY 2014. ICE and the National Protection and Programs Directorate (NPPD) reduced the severity of their significant deficiencies in Budgetary Accounting.

DHS was again able to provide reasonable assurance that our internal controls over financial reporting were operating effectively. We continued to execute our strategy of targeted risk assessment and strong oversight of corrective actions. To continue to build on our progress, we will continue our ongoing remediation efforts along with developing a risk based routine monitoring strategy that will test our key internal controls appropriately across applicable business processes.

The Department's financial systems modernization approach aligns with guidance from the Office of Management and Budget to use shared services where possible, and to split modernization projects into smaller, simpler segments with clear deliverables. USCG, the Transportation Security Administration (TSA) and the Domestic Nuclear Detection Office (DNDO) began efforts to modernize their financial systems in FY 2014 and additional Components are in the planning phase for modernizing their systems. Complementing these efforts are the Department's activities to expand its business intelligence capability to aggregate and report Department-wide financial information to ensure that 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: IT Management and Privacy Issues

DHS remains committed to managing and optimizing DHS IT through a Department-wide IT infrastructure that is reliable, scalable, flexible, maintainable, accessible, secure, meets users' needs, and ensures operational excellence—from the workstation to the data center to the mission application. The Department has set goals to preserve privacy in the execution of homeland security activities by creating appropriate policy assuring that the



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

use of technologies sustain, and do not erode, privacy protections relating to the use of personally identifiable information.

For example, the USCIS Chief Information Officer is revising its Office of Information Technology (OIT) Strategic Plan to ensure it remains up-to-date and relevant in the evolving climate. In addition, USCIS OIT is finalizing a comprehensive refresh strategy that will address plans for updating USCIS's workstations and infrastructure.

Regarding the challenge of sharing and integrating cyber threat information, the NPPD Office of Cybersecurity and Communications (CS&C) issued new Federal Incident Notification Guidelines last month. The revised guidance provides clear instructions for submitting incident notifications to CS&C's United States Computer Emergency Readiness Team (US-CERT) and has been shared with federal government departments and agencies; state, local, tribal, and territorial government entities; information sharing and analysis centers; and foreign, commercial, and private sector organizations. These guidelines support US-CERT in executing mission objectives and result in better quality of information, improved information sharing and situational awareness, and faster incident response times.

Challenge #5: Transportation Security

TSA's commitment to protecting our Nation's transportation systems by ensuring security operations evolve quickly to address new and changing threat environments continues to be one of our highest priorities. TSA continues to work closely with industry trade organizations and our transportation security partners to ensure vital information is shared to enhance transportation security.

During FY 2013, TSA finalized and implemented a strategic plan for the Behavior Detection and Analysis Program, outlining the program mission, vision, and various initiatives being conducted in support of TSA's strategic framework. As a result, OIG agreed to close all remaining open audit recommendations from its related report, including recommendations concerning goals and objectives, training, identifying external partners integral to program success, and developing a financial plan to track expenditures. Regarding OIG's reference to a related U.S. Government Accountability Office (GAO) report, it is important to note that TSA disagreed with GAO's conclusions regarding the scientific validity of TSA's Screening of Passengers by Observation Techniques program. Terrorists pose a persistent and significant threat to transportation and have demonstrated their ability to adapt and innovate to overcome security obstacles. TSA deploys behavior detection protocols because they are based upon sound scientific principles, as validated by a 2011 DHS Science and Technology Directorate study. There



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

is a significant body of research, not referenced in GAO's report, that provides scientific validation for the use of behavior detection protocols.

Challenge #6: Border Security and Immigration Enforcement

DHS continues to strengthen its approach to address the challenges of illegal entry into the United States through a strategy of enhanced intelligence; coordinated operations with federal, state, local, tribal, and international partners; and the ability to respond to changing threats. For example, earlier this year Secretary Johnson directed the creation of a DHS-wide, inter-component campaign plan for the security of the U.S. Southern Border and approaches. The Secretary envisions this plan including a comprehensive strategy and operational plans for the security of the Southern Border, directed at a range of threats and challenges that include illegal migration, illegal drug, human and arms trafficking, the illicit financing of all these operations, and last but not least, the terrorist threat. The Department's Deputy Secretary is overseeing development of the plan, which will be used to guide further analysis by the JRC to develop options for the FY 2017-2021 Program Review Budget.

Regarding the surge of unaccompanied alien children (UAC) in 2014, U.S. Customs and Border Protection (CBP) has already taken many steps to address this issue. For example, CBP deployed Headquarters personnel to the newly developed Unified Coordination Group and embedded them within the four task forces-- Transportation, CBP Holding, Shelter Facilities, and Child Placement. In addition, to alleviate UAC overcrowding in Rio Grande Valley (RGV), CBP opened the Nogales Placement Center (NPC) and temporarily staffed it with more than three hundred Border Patrol Agents focused on supporting surge operations. CBP also worked with its DHS partners to transport 4,593 UAC from the RGV to the new NPC. As confirmed by a recent OIG report on the detention of UAC, CBP has improved its capacity to provide care if the apprehension levels should again increase. Namely, CBP has improved its capacity to provide medical screening, facility cleaning, food service, and case processing for large groups of UAC.

DHS is committed to expediting legal border crossings and creating an environment and infrastructure necessary to enhance legitimate travel and trade. To this end, CBP has improved its Trusted Traveler Programs and continues to work diligently to prevent program abuse. For example, in response to OIG's report on the Secure Electronic Network for Travelers Rapid Inspection program, CBP has worked to implement positive changes regarding procedures, security, internal controls, and information sharing.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Challenge #7: Grants Management

As part of the National Preparedness System, the Federal Emergency Management Agency (FEMA) has developed and is implementing performance assessments that measure progress toward achieving the National Preparedness Goal. FEMA's strategy is to base assessments on the principles that the Nation needs to understand the risks it faces, use those risks to determine the capabilities it needs, assess its current capability levels against those requirements, and track its progress in closing capability gaps.

For example, FEMA has continued to work with those states that have identified challenges with obligating grant funds in a timely manner, reimbursing expenses, and monitoring subgrantee grant management. FEMA has required corrective action plans to develop and implement policies and procedures to ensure compliance with 44 CFR Part 13, and as a result, has been able to reach agreement on closing many OIG recommendations. Additionally, FEMA has taken action to help address procurement and contracting problems by establishing a Disaster Procurement Assistance Team to train Grantees and Subgrantees on avoiding typical pitfalls. FEMA is providing Grantees with state specific audit results to ensure they are equipped with the information necessary to focus efforts, mitigate risks, and reduce vulnerabilities associated with identified problems. FEMA also stood up a Recovery Audit Section as well as an Analytics and Budget Division to ensure it can quickly identify, analyze, and address issues identified by OIG and GAO audits.

Challenge #8: Employee Accountability and Integrity

DHS works hard every day to deter corruption and ensure the integrity of our workforce, as any act of employee corruption interferes with our mission to secure the homeland. Notably, CBP has made significant advancements over the past year in addressing corruption and misconduct. The agency has continued to invest in personnel, technology, programs and training to strengthen integrity, which has resulted in a more resilient CBP. CBP recently released its first unified strategy with respect to integrity, the CBP Integrity and Personal Accountability Strategy ("Integrity Strategy"). This comprehensive Integrity Strategy establishes a unified and multi-layered approach organized around four integrity related mission areas: prevention, detection, investigation, and response to corruption and misconduct. The Integrity Strategy also addresses two primary cross-cutting strategic issues that span all mission areas: integration and awareness. Capitalizing on the synergies and varied capabilities of CBP offices, the Integrity Strategy enhances the Agency's collective ability to address corruption and misconduct in the workforce.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Challenge #9: Infrastructure Protection, Cybersecurity, and Insider Threat

NPPD has begun to implement a single risk assessment methodology with a strategic integrated approach to vulnerabilities and security surveys. This scalable methodology has already been implemented across multiple physical and cyber assessment tools utilized by NPPD's CS&C and Office of Infrastructure Protection establishing a set of core questions and answers to support consistent data collection and enable robust analytics across various sets of physical and cyber security and resilience information. Additionally, the resulting vulnerability studies and security surveys generated by different tools from different sub-components of NPPD are now being compiled within a single interface so as to make them readily searchable and accessible to relevant DHS mission partners. NPPD also deployed an instance of the Cyber Indicator Analysis Platform to the Top Secret Mission Operating Environment network to support CS&C's cyber intrusion prevention capabilities, allowing analysts to create, update, search, import, export, and assign relationships between indicators and sightings.

In addition, DNDO is drafting a standard operating procedure to describe roles and responsibilities for DNDO employees and contractors for safeguarding sensitive information and reporting suspicious activity. At the same time, DNDO is continuing to coordinate with the DHS Office of the Chief Information Security Officer to expand DHS Sensitive Systems Policy guidance regarding protection of intellectual property. Additionally, DNDO affirmed that it has no systems under its direct control which have portable media ports, and in the future, if DNDO has systems under its direct control with portable media ports, it will disable those media ports as recommended. Lastly, DNDO has coordinated with the DHS Office of the Chief Information Officer to conduct assessments to identify wireless devices having unauthorized connections to the DHS enterprise information technology environment.

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 2014 Annual Financial Report¹, 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>



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix C
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy 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
Under Secretary for Management
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, as appropriate

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](https://twitter.com/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