Department of Homeland Security

Office of Inspector General

Major Management and Performance Challenges Facing the Department of Homeland Security

OIG-14-17

December 2013

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

DEC 11 2013

MEMORANDUM FOR: The Honorable Rand Beers
Acting Secretary

FROM: Charles K. Edwards
Deputy 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*, for inclusion in the Department of Homeland Security 2013 *Annual Financial Report*.

Please call me with any questions, or your staff may contact Anne L. Richards, 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) 2013 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 the Department as a whole, as well as every Component. 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 guiding acquisitions, financial systems and reporting, information technology (IT) assets, and cybersecurity. In addition to these challenges, DHS' mission to protect the Nation from domestic and international threats and respond to natural and manmade disasters is challenged by the unpredictable nature of these hazards. Thus, DHS must overcome the challenges inherent to coalescing into "One DHS," as well as those created by factors over which it has little control, but must nevertheless confront to protect our transportation systems and borders and prepare for and recover from threats and disasters.

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

- DHS Operations Integration
- Acquisition Management
- Financial Management
- IT Management and Cybersecurity
- Transportation Security
- Border Security
- Grants Management
- Employee Accountability and Integrity
- Infrastructure Protection

Background

A secure homeland is envisioned as a Nation that is safely protected from terrorism, as well as other manmade and natural hazards, but is also able to respond resiliently if necessary. DHS' FY 2013 budget, including supplemental funding for Hurricane Sandy, was about $72 billion. In its February 2010 report to Congress, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*, the Department 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; and
5. Ensure resilience to disasters.

These missions and their associated goals and objectives specify measures to prevent, protect, respond and recover, build in security to ensure resilience, and facilitate lawful international trade and travel. To mature and strengthen homeland security, the Department has taken significant steps to create a unified and integrated organization that will enhance its performance by focusing on accountability, efficiency, transparency, and leadership development.

DHS Operations Integration

Since its formation in November 2002, DHS has struggled to become fully integrated. With 22 Components and a range of missions, cooperation and coordination continue to be a challenge. The Department's structure sometimes leads to "stovepiping"—Components operating independently and management often not cooperating and sharing information to benefit "One DHS." In 2007, the Secretary affirmed the need for increased cooperation and information-sharing across all DHS Components. Yet, audits conducted in 2012 and 2013 by both OIG and the U.S. Government Accountability Office (GAO) showed that joint requirements development is a persistent challenge for the Department.

FY 2013 Observations

During our recent audits, we identified several programs in which there was little or no cross-component coordination and communication and weak department-level authority. These led to cost inefficiencies and ineffective program management.

Therefore, we made recommendations to enhance collaboration to improve both efficiency and effectiveness.

During an audit of U.S. Customs and Border Protection's (CBP) H-60 helicopter program, we noted that increased cooperation between CBP and the United States Coast Guard (USCG) in managing aviation assets would reduce redundancies and potentially save millions of dollars. Our audit showed that CBP did not properly oversee and manage the acquisition, conversion, and modification of its H-60 helicopters, which affected the cost-effectiveness and timely delivery of the converted and modified H-60s. If CBP were to complete the conversions and modifications at a USCG facility, it would save about $126 million and H-60s would fly 7 years sooner. We made recommendations to improve the Department's management and oversight of its aviation assets, as well as CBP's aviation acquisitions and its H-60 program. The Department disagreed with the potential cost savings and is conducting a study to help determine the most cost-effective approach.

In our audit of CBP's and U.S. Immigration and Customs Enforcement's (ICE) efforts to monitor and detect illegal cross-border tunnels, we reported that although CBP is creating a program to address capability gaps in countering the cross-border tunnel threat, it has not demonstrated how its detection strategy will consider ICE's needs. Without taking into account both Components' needs, the Department risks not being able to disrupt criminal organizations that engage in cross-border smuggling. Our recommendations were designed to improve consideration of the needs of both CBP and ICE and improve DHS' coordination and oversight of counter-tunnel efforts.

In our audit of interoperable communications, we determined that DHS did not establish an effective governing structure with the authority and responsibility to oversee achievement of department-wide, interoperable radio communications. Thus, the Department had limited interoperability policies and procedures, and Component personnel may encounter limitations on communicating with each other. Until the Department develops an effective governing structure and makes a concerted effort to attain interoperability, progress will remain limited. We made two recommendations to improve DHS' oversight of radio communications.

Other audits also showed that DHS could better integrate its program management through enhanced coordination and communication among Components and stronger department-level governance. Overcoming these challenges is critical to improving effectiveness and efficiency and preventing waste and abuse.

Management Progress and Next Steps

In September 2012, GAO reported that DHS had made progress addressing management challenges and that senior officials had demonstrated commitment to addressing them. According to DHS, it made strides in strengthening and integrating its management by establishing common policies, procedures, and systems for some management functions. In addition, the Department has taken steps to standardize operating guidelines, policies, structures, and program oversight; and to integrate data from disparate sources for timely and reliable dissemination of information.

DHS needs to continue the progress it has made in integrating its management functions, as well as take additional actions to further and more effectively integrate across all Components. For example, DHS should continue to implement Integrated Investment Life Cycle Management (IILCM), a transformational concept that integrates all phases of the $60 billion budget and investment management process. IILCM synchronizes Component coordination and investments and integrates decision making and data through business intelligence. By providing critical linkages among strategy, capabilities and requirements analysis, programming and budgeting, and investment oversight, IILCM will shift the paradigm from "budget driving strategy" to "strategy driving budget." Once fully operational, IILCM will allow senior-level decision makers to prioritize, align and measure the progress of investments against mission needs. Engaging in integration efforts such as IILCM is crucial to achieving the Department's mission and truly becoming "One DHS."

Acquisition Management

Efficient and effective acquisition management that complies with Federal regulations, policies, and procedures is critical to preventing waste and abuse and to ensuring that goods and services are procured in a timely manner and at a reasonable cost. The Department continues to be challenged by the complexity and breadth of its acquisitions. The FY 2013 Major Acquisition Oversight List contains 123 programs, 88 of which are Level 1 or Level 2 programs (those with lifecycle costs estimated at $300 million or above or having special departmental interest). Although DHS has established processes and entities to manage acquisitions, it continues to face challenges in its ability to properly coordinate and provide effective oversight of the myriad of acquisitions planned and undertaken by its Components.

FY 2013 Observations

Several audits conducted in FY 2013 illustrate that DHS continues to face challenges in ensuring compliance with its acquisition-related policies and procedures; thorough acquisition planning, including lifecycle management and deployment strategies; and coordination among Components to ensure cost-efficient acquisitions that meet program needs.

For example, DHS has 62 H-60 helicopters operated by CBP and the USCG, both of which are converting them to add about 15 years of operational life. Through an audit of the H-60 program, we determined that DHS did not properly oversee CBP's acquisition of its H-60s. Although the Department had processes and procedures to govern its aviation assets and provide acquisition oversight, these efforts did not fully coordinate the acquisition, conversion, and modification of aviation assets, and did not control acquisition costs, schedules, or performance. CBP did not take into account guidance from the DHS Office of the Chief Procurement Officer (OCPO) in its H-60 acquisition planning. In addition, the DHS Office of Program Accountability and Risk Management (PARM) did not conduct a complete review of CBP's H-60 program because the Department did not ensure that CBP followed departmental acquisition guidance and properly participated in the Acquisition Review Board (ARB) process or coordinated with the ARB.

In an assessment of the Transportation Security Administration's (TSA) deployment and use of advanced imaging technology (AIT) at airports, we determined that the Component did not develop a comprehensive deployment strategy. This occurred because TSA did not have a policy or process requiring program offices to prepare strategic acquisition or deployment plans for new technology that aligned with the overall goals of the Passenger Screening Program. Without documented, approved, comprehensive plans and accurate data on the use of AIT, TSA continued to screen the majority of passengers with walkthrough metal detectors, potentially reducing the technology's security benefits, and possibly inefficiently using resources to purchase and deploy underused AIT units. As a result, TSA potentially reduced AIT's security benefits and may have inefficiently used resources to purchase and deploy the units.

TSA also needs to improve its screening equipment inventory management plans and procedures at its Logistics Center. Specifically, the Component stored unusable or obsolete equipment, did not maintain appropriate safety stock levels, did not have a process to systematically deploy equipment, and did not use all storage space. For example, in 2007, TSA awarded contracts to acquire automated explosive detection systems for baggage screening at airport checkpoints. As of May 2012, TSA had 12 automated explosive detection systems in its warehouse, which, according to one TSA

official, the Component did not plan to deploy. Storing screening equipment for extended periods in warehouses may result in millions of dollars worth of equipment becoming obsolete or unusable. As a result, TSA may be losing the utility of aging equipment and may be able to put the funds used to lease two warehouses to better use.

In our audit of CBP's efforts to acquire cross-border tunnel technology, we noted that the Department has ultimate responsibility for approving CBP's program, allocating resources, and making decisions to counter the tunnel threat.

In September 2012, GAO reported that although DHS had initiated efforts to address the Department's acquisition management challenges, most of its major acquisition programs continue to cost more than expected, take longer to deploy than planned, or deliver less capability than promised. GAO identified 42 DHS programs that experienced cost growth, schedule slips, or both, with 16 of the programs' costs increasing from a total of $19.7 billion in 2008 to $52.2 billion in 2011— an aggregate increase of 166 percent. GAO concluded that DHS recognized the need to implement its acquisition policy more consistently, but that significant work remained. GAO recommended that DHS modify acquisition policy to better reflect key program and portfolio management practices and ensure acquisition programs fully comply with DHS acquisition policy. DHS agreed and, in September 2012, according to officials, it was in the process of revising its policy to more fully reflect key program management practices.

Management Progress and Next Steps

The Department has made progress in its acquisition oversight processes and controls by instituting a life cycle framework to provide acquisition management, support, review, and approval throughout the Department. To strengthen department-wide program management, PARM was created in 2011 and modeled after best practices in the private sector. It continues to provide centralized oversight for all major acquisition programs. Since PARM was established, its effective oversight has resulted in 136 ARBs, 249 Acquisition Decision Memoranda, 3 cancelled major acquisition programs, 8 paused programs, and the removal of program managers when necessary.

The enhanced effectiveness of acquisition oversight is intrinsically linked to the issuance of *Management Directive* (MD 102-01) and the accompanying *Acquisition Instruction Guidebook* (102-01-001), which address many previously identified issues related to acquisition management. According to the Department, PARM is revising MD 102-01 to strengthen acquisition policy implementation instructions and guidebooks by establishing clearer governance requirements and processes for acquisition program management.

MD 102-01 has been institutionalized and is recognized by all Component Executives as the standard acquisition policy roadmap to manage their programs. The ARB has a broad span-of-control and has authorized low risk/high impact programs to proceed to the next phase. The ARB has institutionalized an effective Component Acquisition Executive structure as the single point of accountability for Component programs and also guides managers of major investments through the acquisition governance process.

In the procurement area, the Department has also made some improvements in awarding and managing smaller, "other than full and open competition" contracts. Our review of 40 files related to FY 2012 contracts with a reported value of more than $174 million showed that, compared with previous reviews of noncompetitive contracts awarded during FYs 2008 through 2011, the Department continued to improve its management oversight of acquisition personnel's compliance with policies and procedures. However, these personnel did not always document their consideration of vendors' past performance when researching background on eligible contractors.

DHS reported that PARM has undertaken various initiatives over the last 2 years to improve decision making and provide better insight on the health of the 123 programs on the Major Acquisition Oversight List. For example, PARM developed and implemented the Quarterly Program Accountability Report — a comprehensive, high-level analysis of programs' vital signs that is provided to DHS leadership, Component Acquisition Executives, and program managers.

Going forward, PARM and the ARB should ensure that program managers have completed and clearly documented all acquisition life cycle processes, including fully developing program life cycle cost estimates. The ARB must provide a consistent, department-wide method, using a limited set of key acquisition documents, to evaluate Components' acquisition status and progress at programs' key decision points. By fully implementing the Department's processes and procedures under the appropriate authority level and review, PARM will begin to provide more effective oversight by identifying challenges and controlling cost, schedule, and performance within the Department's acquisition programs.

To improve its acquisition of technologies to detect cross-border tunnels, the Office of Border Patrol determined that it needed to develop a Tunnel Detection and Technology Program to provide the authority and funding CBP needs to develop and acquire technologies. To guide program development, CBP formed an Integrated Product Team, which includes relevant stakeholders and will draft the acquisition planning documents that CBP and DHS require to create a program. According to DHS, CBP is currently in the initial stages of planning and program development. As part of the acquisition process, when the program has sufficient planning to progress in the acquisition lifecycle, it will

come before the acquisition review board for Acquisition Decision Event approval in accordance with MD 102-01.

Financial Management

The Federal Government has a responsibility to be an effective steward of taxpayer dollars. Sound financial practices and related management operations, financial IT 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 minimize inefficient and wasteful spending, make informed decisions to manage government programs, and implement its policies. An effective internal control structure is integral to an organization's management and provides a framework for effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations.

FY 2013 Observations

DHS obtained an unmodified (clean) opinion on all financial statements in FY 2013, a significant accomplishment. Achieving this opinion took considerable manual effort to overcome deficiencies in internal control and a lack of financial IT systems functionality. DHS now has a solid foundation with a full set of audited financial statements; it must now focus on the factors that may jeopardize the sustainability of the financial statement opinion.

In FY 2012, the independent auditors identified five material weaknesses in internal control, which were reduced to four material weaknesses in FY 2013. The four FY 2013 material weaknesses were in financial reporting; IT controls and financial systems functionality; property, plant, and equipment; and budgetary accounting. Management also reported the same four material weaknesses in the Secretary's Assurance Statement, as required by the Office of Management and Budget's (OMB) Circular A-123, *Management's Responsibility for Internal Control*. The Department received an adverse opinion on internal control over financial reporting because of the four material weaknesses.

In FY 2012, the USCG, ICE, and TSA contributed to a material weakness in financial reporting; this material weakness was repeated in FY 2013. Although some findings reported in FY 2012 were corrected, other findings at the USCG and ICE remained in FY 2013. Also in FY 2013, new findings in financial reporting were identified at the

Management Directorate (MGMT), the National Protection and Programs Directorate (NPPD), United States Secret Service (USSS), and Office of Financial Management (OFM). As in previous years, the auditors reported that the USCG does not have properly designed, implemented, and effective policies, procedures, and controls surrounding its financial reporting process. The USCG uses three general ledgers with significant functional limitations that affect its ability to address internal control weaknesses.

In recent years, MGMT and NPPD have assumed more responsibilities for financial management functions to manage their operations and budgets. However, the directorates have not fully designed internal controls to ensure effective monitoring of decentralized operations, and ensure adequate communication with the service provider. Furthermore, they have not fully established a financial management infrastructure, including defined roles and responsibilities that ensure consistently reliable, accurate, and timely reporting for all significant processes. ICE made significant progress addressing deficiencies reported in FY 2012, but in FY 2013, did not fully develop its policies and procedures and its internal controls over financial reporting. The USSS and OFM had several controls that were not operating effectively, which resulted in errors and required adjustments to the financial statements.

A material weakness in IT controls and systems functionality remained in FY 2013. Although 45 percent of the prior-year findings in this area were closed in FY 2013, new findings were identified at all DHS components, with CBP having the greatest number of new findings. The auditors continued to note that many key DHS financial systems are not compliant with Federal financial management system requirements, as defined in the *Federal Financial Management Improvement Act of 1996* and OMB Circular A-127, *Financial Management Systems* (Revised). Limitations in financial systems functionality add substantially to the Department's challenge in addressing systemic internal control weaknesses, and limit the Department's ability to leverage IT systems to process and report financial data efficiently and effectively.

A material weakness in property, plant, and equipment was also repeated in FY 2013. DHS' capital assets consist of items such as property, plant, and equipment (PP&E) operating materials, as well as supplies such as the USCG's boats and vessels, TSA's passenger and baggage screening equipment, and CBP's equipment for patrolling U.S. borders. The USCG maintains approximately 50 percent of DHS' PP&E. In FY 2013, the Component completed several phases of a multiyear remediation plan aimed at producing a full set of auditable financial statements by addressing process and control deficiencies related to its $7.9 billion net worth of PP&E assets. The USCG did not complete some of the remediation efforts until late in FY 2013 and has ongoing remediation activities scheduled for FY 2014, which include plans to fully implement policies and procedures for personal property, construction in process, real property,

internal-use software, buildings, leasehold improvements, and inventory. The auditors also noted that CBP does not consistently adhere to policies and procedures to properly account for asset purchases, construction, depreciation, or disposal of assets in a timely manner.

The auditors identified a material weakness in budgetary accounting again in FY 2013. DHS has numerous sources and types of budget authority, including annual, multiyear, no-year, and permanent and indefinite appropriations, as well as several revolving, special, and trust funds. Timely and accurate accounting for budgetary transactions is essential to managing Department funds and preventing overspending. In FY 2013, the USCG, the Federal Emergency Management Agency (FEMA), ICE, and MGMT continued to improve their policies and procedures for budgetary accounting processes; however, some control deficiencies reported in FY 2012 remained and new deficiencies were identified. These included deficiencies in accounting for undelivered orders, management review of monthly reconciliations, and in IT controls intended to prevent the receipt of goods and services in excess of the obligation. In addition, NPPD has not fully implemented policies and procedures for its processes to obligate and manage funds.

In FY 2014 and beyond, DHS' continuing challenge will be to sustain its progress in achieving an unmodified opinion on its financial statements. The Department relies heavily on manual processes, including internal controls, to produce auditable financial statements; it also relies on manual data calls to its Components' program offices to collect cost information. DHS must use many manual processes because the current legacy financial IT systems do not have the functionality to support implementing more reliable IT application controls. Further remediation of existing internal control weaknesses will likely depend on even greater use of manual processes and on a patchwork of IT systems—perhaps leading to a more unstable financial reporting environment. Toward the end of the financial statement audit, the Department lost a number of key financial leadership personnel which pose a risk to maintain oversight and management review throughout the next fiscal year.

Management Progress and Next Steps

In the past fiscal year, 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 management. DHS reduced its material weaknesses from five to four in FY 2013, and it has a plan to eliminate all material weaknesses by FY 2016.

As reported in the past, a majority of DHS financial systems are outdated and need modernizing. According to the Department, it has launched the Financial Systems Modernization initiative to expand business intelligence capabilities and modernize financial systems where needed. DHS reports that through the Financial Systems Modernization initiative it will be able to manage its resources better, provide enterprise-level information more quickly to support critical decision making, reduce costs by eliminating redundant or nonconforming systems, and promote good business practices through standardization of processes and data where possible.

IT Management and Cybersecurity

In its management of IT processes and procedures, DHS and its Components continue to be challenged by continuity and contingency planning for mission essential functions and operations, protecting against the risk of insider threats, and proper use of social media. In addition, because technology is constantly evolving, protecting the Department's IT infrastructure through cybersecurity is an increasingly important challenge.

FY 2013 Observations

Lessons learned from catastrophic events, such as the attacks of September 11, 2001, Hurricane Katrina in 2005, and Hurricane Sandy in 2012, demonstrate the need to incorporate continuity and contingency in day-to-day planning. Yet, continuity and contingency planning continue to be a challenge for the Department partially because the DHS Office of the Chief Information Officer (OCIO) has not prepared an IT Disaster Recovery Plan to transition headquarters critical information systems and communication assets to an alternate site. Additionally, OCIO did not develop a business impact analysis to identify its mission essential functions or establish policy for the Components to identify critical information assets and mission essential systems. Because of these issues, all seven of the Department's enterprise mission essential systems reviewed appear at risk of not being able to restore essential business functions if disrupted, or to quickly resume normal operations. Without effective IT continuity and contingency planning, mission essential functions and operations are at risk and could be significantly impacted in the event of a severe or catastrophic event.

Trusted insiders (DHS employees) are the greatest threat to loss, theft, or destruction of mission critical data because their job duties or status in the organization give them unfettered or elevated access to mission critical assets. These employees are thoroughly familiar with weaknesses in organizational policies and procedures, as well as physical

and technical vulnerabilities in computer networks and information systems. Through audits of insider threat risk at TSA and CBP, we determined that both Components had made progress in addressing insider threats, but both also needed to strengthen their programs.

Through our review of DHS' use of social media, we also determined that because DHS does not maintain a complete inventory of social media accounts, some employees obtained access outside of the authorization process. In addition, not all Components using social media have adequate guidelines or policies to prevent unauthorized or inappropriate uses of the technologies. There is no formal mechanism for sharing department-wide best practices for using social media platforms; therefore, DHS stakeholders do not understand how social media could be used more effectively to meet mission needs.

In July 2010, the Office of Management and Budget assigned DHS primary responsibility for overseeing the Federal government-wide information security programs. Subsequently, the National Protection and Programs Directorate Office of Cybersecurity and Communications (CS&C) assumed additional cybersecurity responsibilities, and in mid-2012 was reorganized in an effort to promote security, resiliency, and reliability of the Nation's cyber and communications infrastructure. In our audit of CS&C's Federal Network Resilience (FNR) division, we reported that the division has taken actions to address its assigned responsibilities and to improve the information security posture at government agencies. However, NPPD can make further improvements to address its additional cybersecurity responsibilities.

Management Progress and Next Steps

OCIO has taken steps to mature IT management functions, improve IT governance, and integrate IT infrastructure through increased oversight and authority and by reviewing Component IT programs and acquisitions. These steps have enabled DHS to focus on improving continuity and contingency planning, address insider threats, cybersecurity, and use of social media.

DHS has made progress in implementing effective disaster recovery capabilities at the Department's two enterprise data centers. First, it established a list of disaster recovery services that DHS Components can procure for their systems. Second, the enterprise data centers now have disaster recovery regions that provide backup capabilities to allow continued minimum operations in the event of a disaster. To improve in this area, DHS should develop an IT Disaster Recovery Plan that includes a process to transition headquarters-critical information systems and communications assets from a primary location to an alternate location. The Department should perform a business impact

analysis of the OCIO's mission essential function and update the plan every 2 years, develop policies and processes to monitor the availability of all mission essential systems, and develop and implement a process to maintain backup data for enterprise mission essential systems.

U.S. Citizenship and Immigration Services (USCIS), TSA, and CBP have begun to establish collaborative Insider Threat Working Groups to develop an integrated strategy and program to address insider threat risk. They are also beginning to incorporate insider threat vulnerability assessments at selected airports, border locations, and offsite offices. These Components are also checking privileged user accounts on unclassified information systems to verify the necessity for privileged user access and determine user rights granted to system administrators. Finally, the Components are establishing Security Operations Centers responsible for monitoring of information systems to help detect and respond to insider threat incidents. TSA, CBP, and USCIS can further develop their insider threat program by implementing specific policies and procedures, a risk management plan, and enhance existing component-wide training and awareness programs. DHS can strengthen its situational awareness against insider threats by centrally monitoring information systems and by augmenting current IT applications and controls to better detect or prevent instances of unauthorized removal or transmission of sensitive information outside of DHS networks.

DHS has steadily increased its use of various social media sites over the past 5 years. All seven operational Components have established accounts on commonly used social media sites, and public affairs employees have had wide success using these sites to share information and conduct public outreach efforts. These initiatives were effectively managed and administered by department- and component-level public affairs offices. In addition, Component public affairs offices have implemented policies and procedures to provide guidance to employees. However, the Department should communicate the process to gain access to social media and establish a list of approved social media accounts. In addition, DHS needs to complete a department-wide social media policy to provide legal, privacy, and information security guidelines for approved uses. Finally, the Department should require Components to develop and implement social media policies and establish a forum to collaborate and make decisions on the use of social media tools.

To fulfill its cybersecurity responsibilities, FNR manages the annual *Federal Information Security Management Act of 2002* (FISMA), as amended, reporting process and actively evaluates Federal agencies' compliance with the President's cybersecurity initiatives. The division also conducts information security assessments at selected agencies. According to the Department, FNR is coordinating with OMB and through the interagency Joint Continuous Monitoring Working Group to finalize a FISMA strategic

approach, which aligns with and provides authority for FNR's Continuous Diagnostics and Mitigation (CDM) program. FNR is actively engaged in a strategic planning effort under the working title of the FISMA Transformation Project that will define a 3-year plan to redefine the methods for developing FISMA metrics questions, data collection, and data correlation. Furthermore, this project will look to align FISMA requirements with emerging technologies to take full advantage of CDM and related efforts, and develop the functional and business requirements that will be leveraged for the CDM dashboard to meet the information needs of the current DHS stakeholders.

To improve this program, IT management should increase communication and coordination with government agencies, which would improve the FISMA reporting process. NPPD must also address deficiencies in maintaining and tracking the training records of CyberScope contractor personnel and implement the required DHS baseline configuration settings.

Transportation Security

TSA is charged with protecting the Nation's transportation systems to ensure freedom of movement for people and commerce. For airport security, TSA uses various technologies 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. As TSA refines its layers of security and the efficiency of its operations, it must continue to ensure that its operations evolve to address new and changing threat environments.

FY 2013 Observations

In carrying out its mission to provide effective and efficient security measures at airports, TSA continues to face challenges in ensuring the efficacy of these measures and using staff and resources efficiently.

Using covert methods, we tested whether TSA's airport access controls and passenger and baggage screening was effective in preventing unauthorized access to secured areas and whether personnel complied with security requirements. We also used covert testing to evaluate the effectiveness of TSA's AIT units used at passenger screening checkpoints and to determine whether Transportation Security Officers (TSO) followed established policies and procedures for using AIT. We identified access control and checkpoint screening vulnerabilities and made recommendations to strengthen the

effectiveness of access controls. The results of our testing are classified, but were shared with the Department, TSA, and appropriate congressional committees.

Our audit of the Aviation Channeling Services Provider project showed that to address a backlog in background checks of airport ID applicants, TSA temporarily allowed airports to issue badges without the required checks. As a result, some individuals with criminal records were issued badges. This occurred in part because, during the projects implementation, TSA did not document a project plan, roles and responsibilities, budget and spending, and major decisions. It also did not establish and enforce standard testing requirements to identify problems prior to deploying the system for channeling aviation services. TSA also did not implement a strategic plan to ensure the success of the Screening of Passengers by Observation Techniques (SPOT) program. Specifically, it did not assess program effectiveness, have a comprehensive training program, ensure outreach to its partners, or have a financial plan. As a result, TSA cannot ensure that it is screening airport passengers objectively or that the program is cost-effective; it also cannot reasonably justify its expansion.

In our audit of TSA's Office of Inspection, we determined that the office did not use its staff and resources efficiently to conduct cost-effective inspections, internal reviews, and covert testing. Criminal investigators in the office may not have met the Federal workload requirements to receive premium pay, and they performed work that could have been done by other personnel at a lower cost. The office also did not properly plan its work and resource needs, track project costs, or measure performance effectively. In its report on TSA's monitoring of employee misconduct, GAO noted weaknesses in verifying TSA airport staff compliance with policies and procedures for adjudicating misconduct, recording information on adjudication decisions, tracking of time to complete investigations and adjudications, and identifying allegations not adjudicated.

Management Progress and Next Steps

TSA has taken actions to comply with our recommendations. For example, the Component continues to use AIT units more effectively and has developed more AIT training for TSOs. For the Aviation Channeling Services Provider project, TSA developed lessons learned and established a policy requiring comprehensive plans for all projects. Additionally, to improve the SPOT program, TSA is updating its strategic plan and has implemented a training plan for Behavior Detection Officers, which included plans to regularly assess their performance and ensure they are used cost-effectively.

According to the Department, TSA is also taking active steps to strengthen areas identified as needing improvement in response to GAO's report on TSA's monitoring of employee misconduct. TSA concurred with GAO's recommendations and is putting

measures in place to address each of these areas. For example, on August 23, 2013, additional guidance was issued to Employee Relations Users in the Integrated Database to ensure that all corrective and disciplinary actions are recorded in the database. This guidance was also incorporated in the Employee Relations User Guide for the Integrated Database. To further reiterate this guidance, the Assistant Administrator for the Office of Security Operations and the Assistant Administrator for the Office of Human Capital (OHC) will issue a joint memorandum to Federal Security Directors for their support and compliance. On September 19, 2013, during the bi-monthly HRAccess conference call for Administrative Officers/Human Resources Representatives staff members, OHC/ER addressed the additional guidance provided.

TSA needs to continue to improve and regularly assess the efficiency and effectiveness of its personnel and equipment, both of which are critical to protecting our Nation's transportation system. The Component should also further develop comprehensive strategies and program plans aimed at using resources, including personnel, equipment, and IT assets, as efficiently and cost-effectively as possible.

Border Security

DHS' multi-layered effort to secure the Nation's borders is undertaken by CBP, the USCG, and ICE. Together, these Components seek to deter, detect, and interdict illegal entry of people and contraband into the United States, across U.S. land borders and sea frontiers and through our air space. In their mission to protect the Nation, these DHS Components cannot simply sustain their current efforts, but must be prepared to face and overcome numerous, different border security challenges. Improvements in one area often lead individuals and organizations to alter and create new methods to evade security and illegally breach our borders. As long as the United States remains an economically desirable destination to live and work, and a market for illegal drugs, these challenges will remain. Thus, DHS, and in particular the three Components involved in border security, cannot simply maintain the current security posture. The Department must continually develop new and better methods, using both technology and manpower, to interdict illegal entry into the United States by land, air, and sea.

FY 2013 Observations

Recent border security-related audits by OIG and GAO have focused primarily on CBP's role. Specifically, GAO and OIG noted that CBP is challenged in its ability to measure its performance and effectiveness, its technological capability to detect illicit cross-border tunnels, and in its use of air and marine assets.

Although in the past DHS has used the number of apprehensions on the southwest border as an interim goal and measure, GAO testified that this interim measure provides information on activity levels not program results and, therefore, limits DHS and congressional oversight. According to GAO, the Office of Border Patrol, in developing key elements of its FYs 2012 through 2016 Strategic Plan, did not identify milestones and timeframes for developing and implementing performance goals and measures in accordance with standard program management practices. GAO also stated that differences in data collection methods and reporting preclude the Border Patrol from comparing the overall effectiveness of each sector's deployment of border security resources.

Illicit cross-border tunnels along the southwest border are primarily used by criminals to transport illegal drugs into the United States, and they are a significant and growing threat to border security. In an effort to counter this threat, CBP has modified its operations through patrols, intelligence gathering, and closing of illicit cross-border tunnels, but it does not yet have the technological capability to detect the tunnels routinely and accurately. To best address this capability gap, CBP needs to develop and acquire tunnel detection technology, but it has not been able to identify existing technology that functions effectively in its operating environment.

To facilitate their maximum effectiveness and use, CBP needs the right mix of air and marine assets in the right places. GAO's analysis of CBP's Office of Air and Marine's (OAM) FY 2010 performance results indicated that OAM did not meet its national performance goal to fulfill greater than 95 percent of Border Patrol air support requests and did not provide higher rates of support in locations designated as high priority based on threats. One high-priority Border Patrol sector had the fifth highest support rate of all nine sectors on the southwest border. Reassessing the mix and placement of its air and marine assets and personnel and using performance results to make informed decisions could benefit OAM's performance.

Management Progress and Next Steps

In response to GAO's and OIG's recommendations, CBP has begun to address these challenges. However, the Component needs to continue its work.

In May 2012, CBP's Office of Border Patrol issued the *2012-2016 Border Patrol Strategic Plan*, which emphasizes using intelligence information to establish risk relative to threats of cross-border terrorism, drug smuggling, and illegal migration. Under the plan, the Office of Border Patrol intends to continuously evaluate border security by analyzing changes in risk levels against available capabilities across border locations. The Office of Border Patrol is developing performance goals and measures that can be linked to these

new risk assessments and anticipates their publication by the end of 2013. Guidance from September 2012 provides a more consistent, standardized approach for collecting and reporting information that could be used to analyze sector performance and identify capability gaps, allowing for more informed decisions regarding resource deployment for our Nation's borders.

CBP is creating a Tunnel Detection and Technology Program to address capability gaps in countering the cross-border tunnel threat. As part of this effort, CBP is drafting the documents required by DHS to fund, develop, and acquire tunnel detection technology. Additionally, CBP plans to establish a Program Management Office to provide leadership, strategy, and organization to department-wide, counter-tunnel efforts.

In transitioning to a new risk-based approach under the 2012-2016 Border Patrol Strategic Plan, the Office of Border Patrol has begun strategic and technological initiatives that will likely affect the type and level of OAM support and the mix and placement of resources across locations.

In addition, CBP needs to establish milestones and time frames for developing performance goals that define the border security or risk levels to be achieved. These milestones and time frames could improve accountability and oversight of the agency's border security efforts.

Tunnel detection technology needs to address the mission needs of both CBP and the Office of Homeland Security Investigations at ICE because they are responsible for combating cross-border tunnels. Although the CBP Program Management Office seeks to provide leadership, strategy, and organization to DHS tunnel threat efforts, it cannot decide the best way to assign counter-tunnel resources outside of CBP. A departmentally designated authority is needed to make these strategic decisions regarding counter-tunnel policies and procedures.

Also, OAM could benefit from taking additional steps to better ensure that its mix and placement of resources meets mission needs and addresses threats. In addition, DHS could assess potential actions to improve coordination of air and marine activities, better leverage existing resources, eliminate unnecessary duplication, and enhance efficiencies.

Grants Management

DHS grants play a significant role in carrying out its mission to prevent, prepare for, protect against, and respond to natural disasters, acts of terrorism, and other manmade

disasters. These grants, totaling $35 billion since 2003, help State, local, and tribal governments, and private nonprofit organizations respond to and recover from major disasters and emergencies, such as hurricanes, floods, and terrorist attacks. Overseeing preparedness and disaster assistance grants continues to challenge DHS because of the varied nature of hazards, the multitude of types of recipients, and the pressure to respond quickly.

Preparedness grants rapidly expanded after 9/11, and States and local governments began to expect continued high levels of funding, but recent grant funding reductions have negatively affected the ability to sustain prior grant-funded efforts. Grants management has also frequently moved around DHS, and has resided at FEMA since Hurricane Katrina in 2007. FEMA has not developed good measures of the grants' effect on overall preparedness, although Congress has repeatedly ordered development of effective measurement systems. Additionally, following a disaster, FEMA must decide whether to fund the repair or replacement of damaged buildings, and the wrong decision can cost taxpayers millions of dollars. In deciding, FEMA faces challenges from Federal, State, and local officials who may demand quick action to replace a facility rather than repair older or obsolete structures.

FY 2013 Observations

This year, both OIG and GAO have testified before Congress on FEMA's continuing challenge to develop a national preparedness system that could help it prioritize preparedness grant funding. Our 10 audits completed in FY 2013 identified areas for both grant recipient and FEMA improvement, such as States' homeland security strategies; obligation of grants; reimbursement to subgrantees for expenditures; and monitoring of subgrantees' performance and financial management, procurements, and property management.

We also identified a variety of problems with disaster grant management and accounting, ineligible and unsupported costs, and noncompliance with Federal contracting requirements. Of the 59 disaster grant audit reports we issued in FY 2012, 54 reports contained 187 recommendations resulting in potential monetary benefits of $415.6 million. This amount included $267.9 million in questioned costs that we recommended FEMA disallow as ineligible or unsupported, and $147.7 million in unused funds that we recommended FEMA deobligate and put to better use. The $415.6 million in potential monetary benefits represents 33 percent of the $1.25 billion we audited, compared with 28 percent in FY 2011, 13 percent in FY 2010, and 15 percent in FY 2009.

In deciding whether to repair or replace a damaged building, in most instances, FEMA uses the "50 Percent Rule," meaning it will replace a facility if the estimated cost to

repair it exceeds 50 percent of the estimated cost to replace it. Previous and ongoing audits have disclosed serious problems with policies and procedures, including decision calculation and review standards, training, and employee qualifications. Because of the complexities of applying the 50 Percent Rule and a lack of adequate policies and procedures, incorrect replacement decisions cost FEMA millions of dollars.

Management Progress and Next Steps

For preparedness grants, FEMA began requiring state and local governments receiving homeland security funding to complete Threat and Hazard Identification and Risk Assessments (THIRA) by December 31, 2012, and, as a part of this process, develop their own capability requirements. In future State Preparedness reports, state officials are to use the capability requirements they identify to assess their capabilities; FEMA will use these reports, along with other sources, to develop the annual National Preparedness Report. In addition, FEMA has concurred with and taken steps to implement or has implemented almost all of our recommendations to improve the management of homeland security grants.

FEMA recognizes the need for better administration of its disaster grant programs and is working to address this challenge. In response to recommendations, FEMA Regional offices are holding states, as grantees, more accountable for effective and efficient grant management. FEMA also started to examine its own policies related to grant management. For example, FEMA implemented a Strategic Funds Management Initiative focused on obligating Public Assistance projects on the basis of the applicant's capacity, resources, and schedule to complete the work, which will free Federal funds for more immediate needs.

FEMA also recognizes the challenges faced in applying the 50 Percent Rule. In response to recommendations in our disaster grant audit reports, some FEMA Regional Offices have strengthened and clarified policies related to making repair-versus-replace decisions.

FEMA faces continued challenges in measuring the effectiveness of preparedness grant funds. THIRA is a self-reporting tool that allows a jurisdiction to understand its threats and hazards and factors that lead to varied impacts. This is a necessary first step to identifying capabilities, capability targets and gaps, and to focus on specific capabilities, but it may not address the overall state-level strategies or priorities. In addition, it may be difficult to combine the results and determine a national level of preparedness. Until FEMA establishes capability requirements and associated performance measures, it may be unable to determine the resources needed to address capability gaps.

FEMA needs to strengthen and clarify its disaster grant program policies and take steps to ensure that they are applied consistently in the field. The Component should also identify and help close gaps inhibiting effective grant and subgrant management. FEMA should oversee grantees and subgrantees to ensure that they follow laws, regulations, and policies throughout the life of the projects.

In August 2012, FEMA Administrator Fugate wrote that he agreed FEMA's current 50 Percent Rule policy and its implementation need significant revisions, and that our audit observations showed the need for better policy, training, and oversight. FEMA needs to develop improved policies, procedures, preparation and review standards, and training programs to prevent the misapplication of the 50 Percent Rule. Taking these steps should also ensure more consistent application of the rule among the 10 FEMA Regions.

Employee Accountability and Integrity

Investigations of departmental employees range throughout the Components and are initiated in response to allegations of wrongdoing such as smuggling, bribery, child pornography, and theft of departmental funds or property. OIG is particularly concerned with the smuggling of people and goods across the Nation's borders. Smuggling continues to be a large-scale business and remains dominated by drug trafficking organizations that seek to systematically corrupt DHS employees to continue their schemes. Within DHS, OIG has the primary authority for investigating allegations of criminal misconduct by DHS employees.

FY 2013 Observations

In FY 2012, we received approximately 17,690 complaints and opened 1,030 investigations. In that same period, 132 of our cases were accepted for prosecution and we achieved 178 convictions and 106 personnel actions. Thus far in FY 2013, we have received 7,868 complaints and have initiated 320 investigations. Also in FY 2013, we have had 76 cases accepted for prosecution and achieved 83 convictions and 41 personnel actions.

A sample of our 2013 casework demonstrates the wide range and scope of unlawful misconduct in which Department employees engage. For example, in one case we learned that a CBP employee was observed meeting with members of a known drug-trafficking organization. Later, he made arrangements with individuals he believed to be smugglers and allowed a vehicle driven by an undercover agent to pass through a border patrol checkpoint without being inspected. He also met with a confidential

informant and received an $8,000 cash bribe payment in an envelope. After we arrested him, he resigned and pleaded guilty to one count of accepting a bribe.

Similarly, we investigated a CBP employee who was accepting bribes to allow narcotics through his inspection lane. We had an agent pose as a narcotics smuggler and pay the employee a series of bribes in exchange for allowing what he believed to be illegal narcotics to enter the United States. He was found guilty of conspiracy and bribery.

This year, a USCIS employee pleaded guilty to possession of child pornography, and was sentenced to 37 months incarceration and 120 months of supervised release. In 2010, the employee seemingly inadvertently provided another employee with a USB thumb drive containing child pornography, and a search of his residence yielded additional images on his home computers. We also arrested a senior ICE law enforcement officer who was involved in child pornography. He was sentenced to 70 months Federal incarceration, followed by 240 months of supervised release.

Additionally, we investigated and arrested a recently retired, former USCG employee who had stolen government-owned electrical equipment valued at approximately $120,000 and sold it on eBay. After his arrest, he pleaded guilty of two counts of mail fraud and was sentenced to 12 months and 1 day incarceration followed by 24 months of supervised release. He was also ordered to pay $127,600 in restitution.

Finally, we engaged in a joint investigation with a local sheriff's department of a Border Patrol Agent who made a traffic stop of a vehicle driven by a woman in a remote location and sexually assaulted her. Following the investigation, the agent resigned and was sentenced to 96 months in State prison.

Management Progress and Next Steps

In the past year, we expanded our outreach and liaison efforts with other DHS internal investigation offices and partnered with them in joint cases whenever feasible. Our close working partnerships allow us to employ a two-tier strategy—we are primarily engaged in investigations of employee criminal misconduct, while the Components focus on investigations of administrative misconduct and preventive measures. Their measures focus on enhanced screening of applicants, including pre-employment polygraph examinations and more thorough background investigation after hiring. They also provide periodic employee integrity and security briefings, which help the workforce recognize corruption signs and dangers. So that everyone may inform us of employee misconduct or otherwise assist us in our mission, we continued to partner with the Department's Office of Civil Rights and Civil Liberties in our continuing

implementation of Executive Order 13166, *Improving Access to Services for Persons with Limited English Proficiency.*

The *Anti-Border Corruption Act of 2010* required that, by January 4, 2013, CBP administer applicant screening polygraph examinations for all law enforcement applicants prior to hiring. CBP reported that this goal was met in October 2012. The Act also requires CBP to initiate timely periodic background reinvestigations of all CBP personnel. CBP reported that 60 percent of applicants who are polygraphed are found to be unsuitable for employment.

Infrastructure Protection

After the 2001 terrorist attacks, the Nation developed a greater awareness that chemical facilities could be sabotaged and materials released, stolen, or used as weapons of mass destruction. The Federal Government has developed and implemented programs aimed at reducing the safety risks and security risks associated with hazardous chemicals. The *Department of Homeland Security Appropriations Act of 2007* established the Chemical Facility Anti-Terrorism Standards (CFATS) program, which allows DHS to regulate chemical facilities that may present a high-level security risk. Within NPPD, Office of Infrastructure Protection, the Infrastructure Security Compliance Division (ISCD) is responsible for implementing CFATS.

FY 2013 Observations

CFATS was established to improve the security of chemical facilities that present high levels of security risk.

According to a DHS, OIG March 2013 report, CFATS program progress has been slowed by inadequate tools, poorly executed processes, and insufficient feedback on facility submissions. In addition, program oversight had been limited, and confusing terminology and the absence of appropriate metrics led to misunderstandings of program progress. ISCD struggled with a reliance on contractors and the inability to provide employees with appropriate training. Overall efforts to implement the program have resulted in systematic noncompliance with sound Federal Government internal controls and fiscal stewardship, and employees perceived that their opinions have been suppressed or met with retaliation. Although we were unable to substantiate any claims of retaliation or suppression of nonconforming opinions, the ISCD work environment and culture fostered this perception.

In April 2013, GAO also released a report on the CFATS Program. GAO concluded that DHS efforts to assess chemical security risk and gather feedback on facility outreach should be strengthened. According to the pace reflected during GAO's review, DHS will take another 7 to 9 years to fully assess site security plans for high-risk facilities.

Management Progress and Next Steps

Despite ISCD's challenges, the regulated community views the CFATS program as necessary in establishing a level playing field across a diverse industry. In addition, ISCD has begun to take steps to improve CFATS program efficiency and effectiveness. It has developed performance metrics to monitor program performance, initiated tasks to improve program-related tools and processes, reduced reliance on contractors, established internal controls to ensure accountability of funds, selected permanent leadership, and developed a strategy for seeking long-term authorization for CFATS.

DHS reported that they have taken action to address recommendations made by the OIG, as well as GAO, concerning the CFATS program. Corrective actions were made to address 9 of the 24 recommendations reported in the OIG's March 2013 report, which resulted in their closure. The remaining recommendations are considered resolved, but will remain open, pending completion of planned corrective actions. Similarly, NPPD is also addressing three recommendations made by GAO in its April 2013 report to better assess risk associated with facilities that use, process, or store chemicals of interest. In support of efforts to close recommendations, DHS has documented all processes relating to the CFATS tiering methodology, and completed both an internal and external peer review of that methodology.

On August 1, 2013, the President signed an Executive Order, "Improving Chemical Facility Safety and Security," to improve the safety and security of chemical facilities and reduce the risks of hazardous chemicals to workers and communities. The Executive Order directs the Federal Government, including DHS, to:

- improve operational coordination with state and local partners;
- enhance Federal agency coordination and information sharing;
- modernize policies, regulations and standards; and
- work with stakeholders to identify best practices.

Given the recent explosion in West, Texas, government reports on programmatic issues, and budget cuts across the Federal Government, some members of Congress have proposed cutting funding for the CFATS program. DHS needs to provide justification for its expenditures and continue working with Congress and private industry to ensure the long-term authorization of the CFATS program. Also, as required by the Executive Order,

DHS must work with other Federal agencies to establish and complete the requirements of the Chemical Facility Safety and Security Working Group. Furthermore, DHS must address the backlog of more than 3,000 facility site security plans that have yet to be reviewed. DHS representatives will also review the CFATS risk methodology, which affects facility tiering.

Appendix A
Relevant Reports

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

Background

- *DHS Budget-in-Brief*, Fiscal Year 2014, page. 15/220. http://www.dhs.gov/sites/default/files/publications/MGMT/FY%202014%20BIB%20-%20FINAL%20-508%20Formatted%20%284%29.pdf
- DHS, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*, February 2010. http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf
- Letter to The Honorable Benjamin L. Cardin, Co-Chair, Bicameral Task Force on Climate Change, April 17, 2013. (not published)

DHS Operations Integration

- DHS-OIG, *DHS' H-60 Helicopter Programs* (OIG-13-89, May 2013). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-89_May13.pdf
- DHS-OIG, *CBP's Strategy to Address Illicit Cross-Border Tunnels* (OIG-12-132, September 2012). http://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-132_Sep12.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
- GAO, *Continued Progress Made Improving and Integrating Management Areas, but More Work Remains* (GAO-12-1041T, September 2012). http://www.gao.gov/assets/650/648629.pdf
- GAO, *High-Risk Series, An Update* (GAO-13-283, February 2013). http://www.gao.gov/assets/660/652133.pdf

Acquisition Management Challenges

- DHS-OIG, *DHS' H-60 Helicopter Programs* (OIG-13-89, May 2013). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-89_May13.pdf
- DHS-OIG, *Transportation Security Administration's Deployment and Use of Advanced Imaging Technology* (OIG-13-120, September 2013). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-120_Sep13.pdf"

- DHS-OIG, *Transportation Security Administration Logistics Center – Inventory Management* (OIG-13-82, April 2013). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-82_Apr13.pdf
- DHS-OIG, *DHS Contracts Awarded Through Other Than Full and Open Competition During Fiscal Year 2012* (OIG-13-36, February 2013). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-36_Feb13.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
- GAO, *DHS and TSA Continue to Face Challenges Developing and Acquiring Screening Technologies* (GAO-13-469T, May 2013). http://www.gao.gov/assets/660/654419.pdf

Financial Management Challenges

- DHS-OIG, *Independent Auditor's Report on DHS' FY 2012 Financial Statements and Internal Control over Financial Reporting* (OIG-13-20, November 2012). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-20_Nov12.pdf

IT Management and Cybersecurity Challenges

- DHS-OIG, *DHS Can Take Actions to Address Its Additional Cybersecurity Responsibilities* (OIG-13-95, June 2013). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-95_Jun13.pdf
- DHS-OIG, *Transportation Security Administration Has Taken Steps To Address the Insider Threat But Challenges Remain* (OIG-12-120, September 2012). http://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-120_Sep12.pdf
- DHS-OIG, *Examining Insider Threat Risk at the U.S. Citizenship and Immigration Services* (OIG-11-33, January 2011). http://www.oig.dhs.gov/assets/Mgmt/OIG_11-33_Jan11.pdf
- DHS-OIG, *U.S. Customs and Border Protection Has Taken Steps To Address Insider Threat, but Challenges Remain*, (OIG-13-118, September 2013). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-118_Sep13.pdf
- DHS-OIG, *DHS Uses Social Media To Enhance Information Sharing and Mission Operations, But Additional Oversight and Guidance Are Needed* (OIG-13-115, September 2013). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-115_Sep13.pdf
- DHS-OIG, DHS Needs to Strengthen Information Technology Continuity and Contingency Planning Capabilities (Redacted) (OIG-13-110, August 2013). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-110_Aug13.pdf

Transportation Security Challenges

- Public Law 107-71, *Aviation and Transportation Security Act*, November 19, 2001. http://www.gpo.gov/fdsys/pkg/PLAW-107publ71/pdf/PLAW-107publ71.pdf
- DHS-OIG, (U) *Covert Testing of Access Controls to Secured Airport Areas* (OIG-12-26, January 2012). http://www.oig.dhs.gov/assets/Mgmt/OIG_SLP_12-26_Jan12.pdf
- DHS-OIG, *TSA's Aviation Channeling Service Provider Project* (OIG-13-42, February 2013). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-42_Feb13.pdf
- DHS-OIG, *TSA Penetration Testing of Advanced Imaging Technology* (OIG-12-06, November 2011). http://www.oig.dhs.gov/assets/Mgmt/OIG_SLR_12-06_Nov11.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 Screening of Passengers by Observation Techniques* (OIG-13-91, May 2013).http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-91_May13.pdf
- DHS-OIG, *Transportation Security Administration Information Technology Management Progress and Challenges* (OIG-13-101, June 2012). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-101_Jun13.pdf
- GAO, *TSA Could Strengthen Oversight of Allegations of Employee Misconduct* (GAO-13-756, July 2013). http://www.gao.gov/assets/660/656381.pdf

Border Security Challenges

- DHS-OIG, *CBP's Strategy to Address Illicit Cross-Border Tunnels* (OIG-12-132, September 2012). http://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-132_Sep12.pdf
- GAO, *Key Elements of New Strategic Plan Not Yet in Place to Inform Border Security Status and Resource Needs* (GAO-13-25, December 2012). http://www.gao.gov/assets/660/650730.pdf
- GAO, *Opportunities Exist to Ensure More Effective Use of DHS's Air and Marine Assets* (GAO-12-518, March 2012*). http*://www.gao.gov/assets/590/589797.pdf
- DHS-OIG, *Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program* (OIG-13-55, March 2013). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-55_Mar13.pdf

Grants Management Challenges

- DHS-OIG, *Annual Report to Congress on States' and Urban Areas' Management of Homeland Security Grant Programs Fiscal Year 2012* (OIG-13-18, December 2012). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-18_Dec12.pdf
- DHS-OIG, *The State of Illinois' Management of Urban Areas Security Initiative Grants Awarded During Fiscal Years 2006 Through 2008* (OIG-13-08, November 2012). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-08_Nov12.pdf
- DHS-OIG, *The Commonwealth of Virginia's Management of State Homeland Security Program and Urban Areas Security Initiative Grants Awarded During Fiscal Years 2008 Through 2010* (OIG-13-10, November 2012). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-10_Nov12.pdf
- DHS-OIG, *The State of Rhode Island's Management of State Homeland Security Program and Urban Areas Security Initiative Grants Awarded During Fiscal Years 2008 Through 2010* (OIG-13-16, December 2012). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-16_Dec12.pdf
- DHS-OIG, *Wisconsin's Management of Homeland Security Program and Urban Areas Security Initiative Grants Awarded During Fiscal Years 2008 Through 2010* (OIG-13-33, January 2013). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-33_Jan13.pdf
- DHS-OIG, *Kentucky's Management of State Homeland Security Program and Urban Areas Security Initiative Grants Awarded Fiscal Years 2008-2010* (OIG-13-41, February 2013). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-41_Feb13.pdf
- DHS-OIG, *Connecticut's Management of Homeland Security Program Grants Awarded During Fiscal Years 2008 Through 2010* (OIG-13-43, February 2013). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-43_Feb13.pdf
- DHS-OIG, *Massachusetts' Management of Homeland Security Grant Program Awards for Fiscal Years 2008 Through 2011* (OIG-13-44, February 2013). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-44_Feb13.pdf
- DHS-OIG, *Indiana's Management of State Homeland Security Program and Urban Areas Security Initiative Grants Awarded During Fiscal Years 2008-2011* (OIG-13-45, February 2013). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-45_Feb13.pdf
- DHS-OIG, *Mississippi's Management of State Homeland Security Program Grants Awarded During Fiscal Years 2008 Through 2010,* (OIG-13-72, April 2013). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-72_Apr13.pdf
- DHS-OIG, *North Carolina's Management of Homeland Security Program Grants Awarded During Fiscal Years 2008 Through 2010* (OIG-13-74, April 2013). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-74_Apr13.pdf
- DHS-OIG, *FEMA Public Assistance Grant Funds Awarded to City of Atascadero, California* (DS-12-07, March 2012). http://www.oig.dhs.gov/assets/GrantReports/OIG_DS-12-07_Mar12.pdf

- DHS-OIG, *FEMA Public Assistance Grant Funds Awarded to Paso Robles Joint Unified School District, California* (DS-12-03, February 2012). http://www.oig.dhs.gov/assets/GrantReports/OIG_DS-12-03_Feb12.pdf
- DHS-OIG, *FEMA Public Assistance Grant Program Funds Awarded to City of Milwaukee, Wisconsin* (DD-12-14, June 2012). http://www.oig.dhs.gov/assets/GrantReports/OIG_DD-12-14_Jun12.pdf
- DHS-OIG, *FEMA Public Assistance Grant Funds Awarded to Ochsner Clinic Foundation, New Orleans, Louisiana* (DD-12-15, June 2012). http://www.oig.dhs.gov/assets/GrantReports/OIG_DD-12-15_Jun12.pdf
- DHS-OIG, *FEMA's Decisions to Replace Rather than Repair Buildings at the University of Iowa* (DD-12-17, June 2012). http://www.oig.dhs.gov/assets/GrantReports/OIG_DD-12-17_Jun12.pdf
- DHS-OIG, *Regional Transit Authority Needs To Insure Equipment or Forgo $62 Million in FEMA Public Assistance Funds, New Orleans, Louisiana* (DD-13-01, November 2012). http://www.oig.dhs.gov/assets/GrantReports/2013/OIG_DD-13-01_Nov12.pdf
- DHS-OIG, *FEMA Improperly Applied the 50 Percent Rule in Its Decision To Pay for the Replacement of the Martinsville High School, Martinsville, Illinois* (DD-13-04, January 2013). http://www.oig.dhs.gov/assets/GrantReports/2013/OIG_DD-13-04_Jan13.pdf
- DHS-OIG, *FEMA Should Recover $8.5 Million of Public Assistance Grant Funds Awarded to the City of Gulfport, Mississippi, for Debris Removal and Emergency Protective Measures – Hurricane Katrina* (DA-13-10, February 2013). http://www.oig.dhs.gov/assets/GrantReports/2013/OIG_DA-13-10_Feb13.pdf
- DHS-OIG, *FEMA Region VI Should Ensure the Cost Effectiveness of Texas Hazard Mitigation Grant Projects* (DD-13-10, May 2013). http://www.oig.dhs.gov/assets/GrantReports/2013/OIG_DD-13-10_May13.pdf
- DHS-OIG, *Capping Report: FY 2012 FEMA Public Assistance and Hazard Mitigation Grant and Subgrant Audits* (OIG-13-90, May 2013). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-90_May13.pdf
- DHS-OIG, *Unneeded Funding and Management Challenges Associated with the FEMA Grant Awarded to Los Angeles County, California: Third Interim Report* (DS-13-10, June 2013). http://www.oig.dhs.gov/assets/GrantReports/2013/OIG_DS-13-10_Jun13.pdf

Employee *Accountability and Integrity Challenges*

- *DHS-OIG, Semi-Annual Report to the Congress, 10/01/2011 – 03/31/2012* http://www.oig.dhs.gov/assets/SAR/OIG_SAR_Oct11_Mar12.pdf
- DHS-OIG, *Semi-Annual Report to the Congress*, *04/01/2012 – 09/30/2012* http://www.oig.dhs.gov/assets/SAR/OIG_SAR_Apr01_Sep12.pdf

- DHS-OIG, *Semi-Annual Report to the Congress*, *10/01/2012 – 03/31/2013* http://www.oig.dhs.gov/assets/SAR/OIG_SAR_Oct12_Mar13.pdf

Infrastructure Protection Challenges

- DHS-OIG, *Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program* (OIG-13-55, March 2013). http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-55_Mar13.pdf

Appendix B
Management Comments to the Draft Report

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

Homeland Security

December 9, 2013

Charles K. Edwards
Deputy Inspector General
Office of Inspector General
U.S. Department of Homeland Security
245 Murray Lane SW, Building 410
Washington, DC 20528

Re: OIG Draft Report: "Major Management and Performance Challenges Facing the Department of Homeland Security" (Project No. 13-145-AUD-NONE)

Dear Mr. Edwards:

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's (OIG's) perspective on the most serious management and performance challenges facing the Department.

DHS is pleased to note OIG's acknowledgement that "the Department has taken significant steps to create a unified and integrated organization that will enhance its performance by focusing on accountability, efficiency, transparency, and leadership development." DHS is committed to strengthening and building upon existing capabilities, enhancing partnerships across all levels of government and with the private sector, streamlining operations, and increasing efficiencies within its five key mission areas: (1) preventing terrorism and enhancing security, (2) securing and managing our borders, (3) enforcing and administering our immigration laws, (4) safeguarding and securing cyberspace, and (5) ensuring resilience to disasters.

DHS missions are complex and highly diverse, necessitating continuous and sustained management attention in order to succeed, while improving the efficiency and effectiveness of its many programs and operations. For example, to support the mission of safeguarding and securing cyberspace, the Department has continued to strengthen both the monitoring of insider threats and its assessments to prevent loss, theft, or destruction of mission-critical data. DHS appreciates the insights OIG provides in support of these mission areas. The following summarizes specific successes and accomplishments in response to the OIG's reported challenges areas.

Challenge #1: DHS Operations Integration

The Department's commitment to strengthening and integrating all 22 Components to become "One DHS" and developing joint requirements is clearly demonstrated through Integrated Investment Life Cycle Management (IILCM). Once implemented, IILCM will integrate all phases of the $60-billion budget and investment management process, providing critical linkages between strategy, capabilities and requirements analysis, programming and budgeting, and

investment oversight. This integrated approach uses portfolio management to eliminate any unnecessary redundancy of requirements, includes executive leadership from across the Department, and mandates close coordination between Components assigned to specific portfolios. Instituting this framework will result in cost-effective resource distribution that is aligned to the Department's strategic goals.

Another example of DHS's commitment to developing joint requirements is illustrated through its efforts to achieve interoperability in the wireless communications arena. Chartered in April 2012, the Joint Wireless Management Office serves as a central collaboration entity and is developing the requirements and architecture framework for combining disparate communications systems. Under this framework, a DHS-wide Communication Interoperability Plan, which will contribute to integration and improve mission effectiveness, is being developed in partnership with Component representatives.

Challenge #2: Acquisition Management

The DHS Office of Program Accountability and Risk Management (PARM) is responsible for the Department's central oversight of acquisition program management and is responsible for managing program governance, program support, and acquisition program management policy. In addition, PARM assesses the health of major acquisitions and works with Components to build program management expertise.

PARM, in conjunction with Component executives, implemented a continuous program review process under a tiered governance model to increase the Department's ability to monitor program execution. In addition to convening 136 Acquisition Review Boards (ARBs) since 2009, PARM has established 13 Executive Steering Committees to ensure that Component Acquisition Executives are engaged to support programs and mitigate risks between formal acquisition reviews by the ARBs. Since PARM was established, its effective oversight has resulted in 249 Acquisition Decision Memoranda, 3 canceled major acquisition programs, 8 paused programs, and the removal of program managers when necessary.

PARM has also taken actions over the last 2 years to improve decision making and provide better insight on the health of 123 major acquisitions listed on the Major Acquisition Oversight List. For example, PARM developed standardized acquisition scorecards to evaluate program readiness to proceed through the acquisition lifecycle. The scorecards leverage best practices and U.S. Government Accountability Office criteria to assess the quality and completeness of acquisition program documentation, using a transparent and repeatable process. In the past 18 months, all new programs have completed required acquisition documentation.

Challenge #3: Financial Management

As the OIG report acknowledges, DHS eliminated its remaining audit qualification and has earned its first-ever, unmodified opinion on all five financial statements. This means that the balances presented in all our financial statements are materially correct. This achievement

demonstrates DHS's sustained financial management progress and commitment to accountability, transparency, and stewardship of taxpayer dollars.

The entire DHS financial management community has made great strides year after year, earning the Department the unmodified opinion. For example, the U.S. Coast Guard made tremendous progress in FY 2013 and was able to remediate their general property, plant, and equipment line item on the Balance Sheet. In addition, the Transportation Security Administration (TSA) successfully remediated its two remaining significant deficiencies during FY 2013.

DHS's efforts are focused on continuing to reduce material weaknesses and significant deficiencies in internal controls over financial reporting. For 2 consecutive years, DHS was able to provide reasonable assurance that our internal controls over financial reporting (ICOFR) were operating effectively. The Department will continue to work on the four remaining material weaknesses identified in the Secretary's Assurance Statement to achieve our goal of obtaining a clean opinion on the ICOFR audit by FY 2016.

Key to the Department's continued progress toward sound financial management and internal controls is the ability of the Components to produce consistent, reliable, and timely financial data. DHS has taken significant steps to modernize Component financial systems where needed, implement a common line of accounting, and maintain data quality standards to sustain audit success. Complementing this effort, DIIS continues to develop a business intelligence solution to collect and aggregate data from Component systems to report Department-wide financial information and 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 missions.

The progress made in financial management at DHS is due to the hard work of dedicated employees at the DHS Office of the Chief Financial Officer and Components across the Department. Working together as One DHS, the financial management community has laid a foundation of sound business processes and standards that will sustain our successes for years to come.

Challenge #4: IT Management and Cybersecurity

As noted by OIG, the Department has made progress in implementing effective disaster recovery capabilities at its enterprise data centers. However, DHS is concerned that OIG did not consider all existing Information Technology (IT) disaster recovery and contingency planning activities, given that these capabilities have been proven during recent disaster events. The Office of the Chief Information Officer (OCIO), in cooperation with the Office of Operations Coordination and Planning (OPS), established continuously operable IT services, a permanent IT support team at its alternate site, and a well-established Emergency Response Group with detailed and documented procedures to activate alternate systems. OCIO is acquiring services to implement automated monitoring capabilities of mission-essential systems, and is also coordinating with OPS to update the business impact analysis of OCIO's mission-essential function. Further, OCIO is consolidating the information from its extensive disaster recovery planning efforts into

a single IT Disaster Recovery Plan for DHS headquarters. Lastly, OCIO has either completed the actions recommended in OIG's report or is in the process of implementing corrective measures.

DHS agrees that Components have made progress to address insider threats. Specifically, TSA's Information Assurance Division implemented a training plan that is routinely used in Insider Threat Assessments to inform and educate after auditing insider activity at airports. TSA also implemented insider threat monitoring capabilities to TSA-controlled Secret and Top Secret networks and established the Classified Security Operations Center. This Center employs analysts and forensics professionals focused on detecting insider activity in networks holding TSA's most sensitive data.

Further, U.S. Citizenship and Immigration Services has made significant progress to address OIG's January 2011 recommendations to strengthen the Department's security posture against malicious insider threats. As of October 2013, 16 of the 18 recommendations have been implemented and closed.

In September 2013, OIG released its report regarding the effectiveness of DHS's use of social media to facilitate information sharing and enhance mission operations. The Department disagreed with OIG's recommendation to require Components to develop and implement social media policies—existing policies already provide guidance for using social media. Specifically, Components are required to complete a form describing the operational use of social media, establish Rules of Behavior for such use, and provide the appropriate training. DHS also noted that it has a list of approved social media accounts for public affairs purposes as well as a DHS-wide list for other purposes.

Challenge #5: Transportation Security

TSA continues to work closely with industry trade organizations and transportation security partners to ensure vital information is shared to increase security and mitigate transportation vulnerabilities. TSA established a policy requiring comprehensive plans for all acquisition programs. It continues working to strengthen existing strategic plans for security programs and continues to evaluate security training programs as well as procedures and programs to increase transportation security.

TSA has taken actions to address OIG's recommendations to improve the efficiency and effectiveness of its vetting systems by developing a fully integrated and scalable enterprise solution for the enrollment, screening, and credentialing of transportation workers. With respect to the Aviation Channeling Services Provider audit, TSA developed lessons learned and established a policy requiring comprehensive plans for all projects.

To improve the Screening of Passengers by Observation Techniques program, TSA has completed and OIG has closed out five out of the six recommendations focused on enhancing the efficiency and effectiveness of its behavior detection and analysis capabilities. TSA has developed and implemented a training plan, a Behavior Detection and Analysis (BDA)

communications plan, and deployed multiple quality assurance controls to include a performance metrics plan to regularly assess program performance and ensure that Behavior Detection Officers are used in a cost-effective manner. TSA also has an approved Strategic Plan for BDA, which has been submitted to OIG for consideration to close OIG's final outstanding open recommendation.

Challenge #6: Border Security

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, U.S. Customs and Border Protection's (CBP's) U.S. Border Patrol (USBP) leverages information sharing, collaboration, and rapid response to secure the Nation's borders against all types of illegal entries in a manner that is risk based, outcome focused, and prioritizes capabilities against the highest threats.

USBP continues to expand its use of the Unified Command, providing a forum for border security partners to share information, integrate resources, and coordinate operations. CBP continues to evolve its network to maximize a "whole of government approach" when it comes to border security. These initiatives aim to identify and disrupt transnational criminal organizations through collaborative law enforcement efforts, allowing USBP and its partners to interdict threats against national security and develop intelligence to mitigate future threats. During FY 2013, these efforts have resulted in the apprehension of over 388,000 individuals and the seizure of almost 2.3 million pounds of narcotics, 570 firearms, and $8.5 million in currency.

Challenge #7: Grants Management

The Federal Emergency Management Agency (FEMA) continues to develop and implement an integrated national preparedness system (NPS) to achieve the capabilities and targets established in the National Preparedness Goal. The Goal defines the 31 core capabilities necessary to prepare for the threats and hazards that pose the greatest risk to the security of the Nation and provides concrete statements of the Nation's requirements for each core capability. The NPS identifies and assesses risks (threats, vulnerabilities, consequences), determines the capabilities needed to address these risks, assesses required capability levels, and provides an approach to planning, building, and sustaining these capabilities.

DHS is continuing work on documenting policies, standard operating procedures, and processes to ensure open competition, prevent Anti-Deficiency Act violations, and comply with congressional notification requirements. FEMA's Office of the Chief Financial Officer is coordinating closely with staff in the DHS Office of the Chief Financial Officer to address corrective actions resulting from the FY 2012 audit of DHS's Financial Statement and Oversight of Internal Controls. A number of milestones with positive impacts on a variety of problems with disaster grant management and accounting are being addressed. Financial reporting by grantees is being examined to find opportunities for improvements and training. DHS is making progress in strengthening internal control procedures related to grant accruals, payment system

reconciliations, and audit resolution and compliance. Scheduled work is underway to add enhancements to grant information systems, allowing collection of project-level data, and regional teams are being established in an effort to resolve ineligible and unsupported costs.

In April 2012, FEMA's Public Assistance (PA) Division published the Public Assistance Program Pocket Guide (the Pocket Guide). The Pocket Guide provides direction on a consistent approach to delivering the PA Program. It describes the fundamentals to be followed in PA field operations nationally in order to streamline processes for more efficient program delivery and provides detailed instructions on critical elements of the Project Worksheet development process. In the last year, PA trained close to 2,300 FEMA, state, and local personnel on consistent implementation of the PA program nationally.

Challenge #8: Employee Accountability and Integrity

CBP has made significant advancements in battling corruption and misconduct internally. CBP conducts background investigations and polygraph examinations of all applicants for law enforcement positions as a way to detect possible issues before an applicant becomes an employee.

Collaboration and information sharing are critical to the effective investigation into allegations of corruption and serious misconduct by DHS employees. As alluded to in OIG's draft report, OIG and CBP have a Memorandum of Understanding (MOU) that allows CBP to provide investigative support upon request to OIG on CBP-related misconduct cases. Similarly, CBP has another MOU with U.S. Immigration and Customs Enforcement (ICE) that allows CBP to partner with ICE to conduct investigations on CBP-related misconduct cases. OIG, ICE, and CBP are working together as partners to investigate these allegations and promote workforce integrity.

Maintaining a culture of integrity must be a priority for every single person working at CBP. It must be an underlying focus for every team, program, and office. CBP is currently developing an Agency-level integrity strategy to address factors involved with possible corruption or other misconduct. CBP's Office of Internal Affairs (IA) cannot be alone in the effort to ensure the integrity of the workforce. For example, the USBP Office of Field Operations and IA have integrated staff that evaluates integrity trends and patterns through analysis of data anomalies at ports of entry and checkpoints. Other efforts include cross-organizational representation in integrity-focused committees.

Challenge #9: Infrastructure Protection

Over the past 18 months, significant progress has been made in advancing the Chemical Facility Anti-Terrorism Standards (CFATS) program. This includes implementation of a revised Site Security Plan (SSP) review process that has dramatically increased the pace of SSP reviews, additional training for inspectors on updated inspection protocols, and the documentation of a number of critical processes through Standard Operating Procedures. As of December 2, 2013, these efforts have enabled the Department to authorize more than 900 security plans, conduct

nearly 600 Authorization Inspections, and approve nearly 400 security plans. The Department is now on pace to authorize and inspect as many as 80 security plans and approve between 30 and 60 security plans per month, and is continuing to explore ways to further increase performance.

Finally, while there is no indication that the incident was a terrorist attack, the Department agrees that the recent explosion at the West, Texas, chemical facility reinforces the need for appropriate security at high-risk chemical facilities. Any facility that manufactures, uses, stores, or distributes certain chemicals above a specified quantity listed in the CFATS Appendix A has 60 days to complete and submit a Top-Screen to DHS. The West, Texas, facility did not submit a Top-Screen. DHS is increasing efforts to identify other facilities that may have similarly failed to submit Top-Screens. These efforts include exchanging lists of facilities with appropriate federal entities and state officials and performing cross-walks of those lists to help identify potentially non-compliant facilities. This is part of DHS's commitment to the successful implementation of Executive Order (EO) 13650 on Improving Chemical Facility Safety and Security. As part of its efforts to enhance federal agency coordination and information sharing as part of the EO, DHS, along with the Department of Labor and the Environmental Protection Agency, is co-chairing a working group focused on implementation of the EO.

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 2013 Annual 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.

Sincerely,

Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

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

Appendix C
Report Distribution

Department of Homeland Security

Acting 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
Acting 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 obtain additional copies of this document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to:

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

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

The OIG seeks to protect the identity of each writer and caller.