Department of Homeland Security

Office of Inspector General

Major Management Challenges Facing the Department of Homeland Security

OIG-12-08

November 2011

Office of Inspector General

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

November 10, 2011

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

The attached report presents our fiscal year 2011 assessment of the major management challenges facing the Department of Homeland Security. As required by the *Reports Consolidation Act of 2000* (Public Law 106-531), we update our assessment of management challenges annually.

We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Charles K. Edwards
Acting Inspector General

Office of Inspector General

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

Major Management Challenges Facing the Department of Homeland Security

At its establishment in 2003, the Department of Homeland Security (DHS) faced the difficult task of building a cohesive, effective, and efficient Department from 22 disparate agencies while simultaneously performing the mission for which it was created. That mission, to secure the nation against the entire range of threats that we face, is itself an arduous assignment. The Department has made progress in coalescing into an effective organization, as well as addressing its key mission areas to secure our nation's borders, increase our readiness and resiliency in the face of a terrorist threat or a natural disaster, and implement increased levels of security in our transportation systems and trade operations.

As in previous years, the Department's major challenges lie in nine broad areas, which we address below:

- Acquisition Management
- Information Technology Management
- Emergency Management
- Grants Management
- Financial Management
- Infrastructure Protection
- Border Security
- Transportation Security
- Trade Operations and Security

ACQUISITION MANAGEMENT

Although the Department continues to make progress in improving its acquisition management, it remains a significant challenge facing DHS, in part because of the magnitude of the number, dollar value, and complexity of its acquisition activity. Below, we identify where DHS improved its acquisition management process, as well as areas where it continues to face challenges.

Organizational Alignment and Leadership

In fiscal year (FY) 2011, DHS improved the acquisition program's organizational alignment and maintained strong executive leadership, but more needs to done. In January, DHS reorganized the reporting structure of the procurement management and program management functions to provide a layered approach to acquisition oversight. Now the Office of the Chief Procurement Officer (OCPO) leads procurement management functions and the Under Secretary for Management leads program management functions. Components continue to maintain their own acquisition and procurement staff. At the component level, the Chief Acquisition Executive is responsible for acquisition program management and the Head of Contracting Activity is responsible for acquisition procurement. There are currently eight chief acquisition executives and nine heads of contracting activity in DHS. The chief acquisition executives and the heads of contracting activity report informally to the Under Secretary for Management and OCPO, respectively.

According to the Government Accountability Office (GAO),[1] DHS has not fully planned for or acquired the workforce needed to implement its acquisition oversight policies. A GAO report issued in February 2011 states that, DHS needs to implement its Integrated Strategy for High Risk Management and continue its efforts to (1) identify and acquire resources needed to achieve key actions and outcomes; (2) implement a program to independently monitor and validate corrective measures; and (3) show measurable, sustainable progress in implementing corrective actions and achieving key outcomes. DHS needs to demonstrate sustained progress in all of these areas to better strengthen and integrate management functions throughout the Department and its components' acquisition functions.

Policies and Processes

DHS continues to develop and strengthen its acquisition management policies and processes. However, the Department needs to further refine its policies to provide detailed guidance, and improve oversight and internal controls in some key areas. For example, the Department needs to improve internal control procedures to mitigate the inherent risks associated with purchase card use. Our review of the Department's purchase card program[2] found that the post-payment audit process did not ensure that component personnel were meeting minimum internal control requirements established by the Office of Management and Budget (OMB). Nor did the process effectively target high-risk transactions. Ninety-three percent of the purchase card transactions we reviewed did not fully comply with OMB requirements, and

[1] GAO-11-278, *High Risk Series - An Update*, February 2011.
[2] DHS-OIG, *Use of DHS Purchase Cards*, (OIG-11-101, August 2011).

the Department's purchase card manual and components' guidance were incomplete and inconsistent. Based on our audit, the Department's Office of the Chief Financial Officer has initiated corrective actions to improve internal controls over the purchase card program.[3]

The Department can also improve management of its use of strategic sourcing. In March 2011, we found that the Department did not have a logistics process in place to facilitate strategic sourcing of detection equipment. Strategic sourcing would require that management standardize equipment purchases for explosive, metal, and radiation detection equipment; identify common mission requirements among components; and develop standard data elements for managing the inventory accounts of detection equipment. Improving its management of detection equipment will offer the Department opportunities to streamline the acquisition process and improve efficiencies.[4]

Although the Federal Emergency Management Agency (FEMA) has developed and strengthened acquisition management policies and processes, it continues to face challenges. Weak internal controls resulted in multi-million dollar contracts with vague and questionable requirements.[5] In addition, task monitors, agency employees responsible for managing and monitoring the contractors, had not received written guidance or training on how to evaluate contractor performance or certify billing invoices. Substantial improvements are needed in FEMA's oversight of contracts, including the prompt implementation of corrective actions.

In response to presidentially-declared disasters, FEMA's Public Assistance-Technical Assistance Contract firms (PA-TACs) provide technical assistance to state, local, and tribal governments awarded grants to fund debris removal and repair structures such as schools, medical facilities, and bridges. The *Brooks Act*[6] requires engineering and architectural firms to be selected based on competency, qualifications, and performance, but FEMA chose between its three PA-TACs with the goal of ensuring the firms were paid equal sums over the life of their FEMA contracts. FEMA had no performance measures for its PA-TACs and failed to monitor or evaluate their performance. FEMA's contract files were not in compliance with regulations. Insufficient oversight of the contracts creates an environment ripe for waste, fraud, and abuse.[7]

Acquisition Workforce

DHS made progress in the recruitment and retention of a workforce capable of managing a complex acquisition program. The number of procurement staff has more than doubled since 2005. In addition, participation in the Acquisition Professional Career Program, which seeks to develop acquisition leaders, increased 62% from 2008 to 2010. Nevertheless, DHS continues to face workforce challenges across the Department.

---

[3] DHS-OIG, *Improving FEMA's Disaster Purchase Card Program*, (OIG-10-91, May 2010).
[4] DHS-OIG, *DHS Department-wide Management of Detection Equipment*, (OIG-11-47, March 2011).
[5] DHS-OIG, *Improving FEMA's Individual Assistance, Technical Assistance Contracts*, (OIG-11-114, September 2011), and *Improvements Needed in FEMA's Management of Public Assistance-Technical Assistance Contracts,* (OIG-11-02, October 2010).
[6] *Brooks Architect-Engineer Act*, 40 U.S.C. §1101, et seq.
[7] DHS-OIG, *Improvements Needed in FEMA's Management of Public Assistance-Technical Assistance Contracts,* (OIG-11-02, October 2010).

According to GAO, the United States Coast Guard (Coast Guard) reduced its acquisition workforce vacancies from approximately 20 percent to 13 percent,[8] and had filled 832 of its 951 acquisition positions as of November 2010. Although acquisition workforce vacancies have decreased, program managers have ongoing concerns about staffing program offices. For example, the HH-65 Aircraft Program Office had only funded and filled 10 positions out of an identified need for 33 positions. Also, according to its August 2010 human-capital staffing study, program managers reported concerns with staffing adequacy in program management and technical areas. To make up for shortfalls in hiring systems engineers and other acquisition workforce positions for its major programs, the Coast Guard uses support contractors, which constituted 25 percent of its acquisition workforce as of November 2010.

FEMA continues to make progress in the recruitment and retention of a workforce capable of managing complex acquisition programs. However, significant challenges remain. Acquisition staff turnover in FEMA has exacerbated file maintenance problems and resulted in multimillion-dollar contracts not being managed effectively or consistently. One of FEMA's challenges is hiring experienced contracting officers to work at disasters. The majority of FEMA staff at a disaster site work on an on-call, intermittent basis. FEMA categorizes all its disaster assistance employees in the occupational series 301, regardless of the function the employee will perform for FEMA. As such, a Disaster Assistance job announcement will not appear in a search for open contracting officer positions, limiting FEMA's ability to attract seasoned contracting officers. Secondly, by being categorized as a 301, Disaster Assistance contracting officers will only be able to administer contracts up to $150,000. Thirdly, the Office of Personnel Management has allowed waivers for retired annuitants who return classified as contracting officers; however, these same waivers are not available to employees classified as 301s. Consequently, Disaster Assistance employees classified as 301s are not encouraged to continue working after the first 120 days after a disaster declaration. This increases turnover, which is detrimental to smooth contract execution.[9]

FEMA has made great strides in improving its contracting officer's technical representatives (COTRs) cadre. FEMA has dedicated staff to oversee the COTR program; developed a tiered system, which ties training requirements to dollar values of contracts a COTR can monitor; and established an intranet site containing tools for COTRs' use. However, many trained COTRs have never been assigned a contract, and are unsure of their ability to be effective doing so. And, although they represent the contracting officer, the COTR's appraisal is completed by their supervisor in their program office, rather than the applicable contractor officer, thus leading to divided loyalties.[10]

[8] GAO-11-480, *Coast Guard: Opportunities Exist to Further Improve Acquisition Management Capabilities*, April 2011.
[9] DHS-OIG, *FEMA's Contracting Officer's Technical Representative Program*, (OIG-11-106, September 2011).
[10] DHS-OIG, *FEMA's Contracting Officer's Technical Representative Program*, (OIG-11-106, September 2011).

Knowledge Management and Information Systems

DHS made progress in deploying an enterprise acquisition information system and tracking key acquisition data. The Department's acquisition reporting system of record, known as nPRS (next-Generation Period Reporting System), tracks components' level 1, 2, and 3 acquisition investments. It also has capabilities to store key acquisition documents, earned value management information, and risk identification. Component personnel are responsible for entering and updating information, which includes cost, budget, performance, and schedule data. However, components did not complete and report all key information in nPRS. In *DHS Oversight of Component Acquisition Programs*,[11] we reported that only 7 of 17 programs (41%) reported Acquisition Program Baseline required milestones. These milestones establish the acquisition cost, schedule, and performance values. Only 13 (76%) programs reviewed contained required key documentation such as a mission needs statement, acquisition plan, operational requirements document, and integrated logistics support plans.

INFORMATION TECHNOLOGY MANAGEMENT

Creating a unified information technology infrastructure for effective integration and agency-wide management of Information Technology (IT) assets and programs remains a challenge for the DHS Chief Information Officer (CIO). The CIO's successful management of IT across the Department will require the implementation of strong IT security controls, coordination of planning and investment activities across DHS components, and a commitment to ensuring privacy.

IT and Cyber Security

During our FY 2010 *Federal Information Security Management Act*[12] (FISMA) evaluation, we reported that the Department continued to improve and strengthen its security program. Specifically, the Department implemented a performance plan to improve on four key areas: Plan of Action and Milestones (POA&Ms) weaknesses remediation, quality of certification and accreditation, annual testing and validation, and security program oversight. Although the Department's efforts have resulted in some improvements, components are still not executing all of the Department's policies, procedures, and practices. Management oversight of the components' implementation of the Department's policies and procedures needs improvement in order for the Department to ensure that all information security weaknesses are tracked and remediated, and to enhance the quality of system certification and accreditation.

Further, over the past year, we have reported on the challenges specific components face in strengthening IT security. For example, in July 2011, we reported that the Transportation Security Administration (TSA) has implemented effective physical and logical security controls to protect its wireless network and devices.[13] However, we identified high-risk

[11] DHS-OIG, *DHS Oversight of Component Acquisition Programs,* (OIG-11-71, April 2011).
[12] Title III of the *E-Government Act of 2002*, Public Law 107-347.
[13] DHS-OIG, *Improvements in Patch and Configuration Management Controls Can Better Protect TSA's Wireless Network and Devices,* (OIG-11-99, July 2011).

vulnerabilities involving TSA's and Federal Air Marshal Service's patch and configuration controls. In September 2011, we reported that U.S. Customs and Border Protection (CBP) needs to strengthen enterprise wireless infrastructure security by remediating its open POA&Ms in a timely manner, enabling the wireless intrusion detection system to protect its network, and by performing regular vulnerability assessments to evaluate the effectiveness of wireless security.[14] In March 2011, we reported on the steps the U.S. Citizenship and Immigration Services (USCIS) needs to take to protect its systems and information from the IT insider threat posed by employees and contractors.[15] Specifically, USCIS needs to institute an enterprise risk management plan and incorporate insider threat risk mitigation strategies into its new business processes, institute a logging strategy to preserve system activities, and consistently enforce employee exit procedures.

In the area of cybersecurity, we reported in June 2011 that the National Protection and Programs Directorate (NPPD) has made progress in sharing cybersecurity threat information and raising cybersecurity awareness.[16] However, significant work remains to address the open actions and recommendations and attain the goals outlined in *The National Strategy to Secure Cyberspace*, National Infrastructure Protection Plan, and Comprehensive National Cybersecurity Initiative. In addition, NPPD must ensure that systems personnel receive required Protected Critical Infrastructure Information training and that configuration and account access vulnerabilities are mitigated to protect the department's critical infrastructure information and sensitive data.

IT Management

Management of IT to ensure that it integrates well with other department-wide systems and federal partner agency systems and that it supports users' needs fully has been a challenge for several components. For example, the United States Coast Guard's command center and partner agency systems are not sufficiently integrated.[17] These limitations had a variety of causes, including technical and cost barriers, aging infrastructure that is difficult to support, and stove-piped system development. As a result, field personnel relied on inefficient workarounds to accomplish their mission. Additionally, the IT systems developed by DHS to share information between DHS and state and local fusion centers did not support their needs fully.[18] For example, the Homeland Security Information Network and the Homeland Security State and Local Community of Interest systems, both developed by DHS, are not integrated. As a result, users must maintain separate accounts, and information cannot easily be shared across the systems. Fusion center personnel also expressed concern that there were too many federal information sharing systems that were not integrated.

---

[14] DHS-OIG, *Security Issues with U.S. Customs and Border Protection's Enterprise Wireless Infrastructure,* (OIG-11-118, September 2011).
[15] DHS-OIG, *Examining Insider Threat Risk at the U.S. Citizenship and Immigration Services (Redacted)* (OIG-11-33, January 2011).
[16] DHS-OIG, *Planning, Management, and Systems Issues Hinder DHS' Efforts To Protect Cyberspace and the Nation's Cyber Infrastructure,* (OIG-11-89, June 2011).
[17] DHS-OIG, *Coast Guard Has Taken Steps To Strengthen Information Technology Management, but Challenges Remain* (OIG-11-108), September 2011).
[18] DHS-OIG, *Information Sharing With Fusion Centers Has Improved, but Information System Challenges Remain* (OIG-11-04, October 2010).

In addition, several components involved in IT transformation activities did not have updated IT strategic plans to help guide IT investments decisions. For example, the U.S. Secret Service's IT strategic plan had not been updated since 2006 and did not reflect and guide its modernization efforts, address identified IT weaknesses, or integrate its IT with the DHS-wide enterprise infrastructure.[19] In addition, FEMA's IT strategic plan was not comprehensive enough to coordinate and prioritize its modernization initiatives and IT projects.[20] The plan did not include clearly defined goals and objectives, nor did it address program office IT strategic goals.

DHS and its components also face challenges in upgrading their respective IT infrastructures, both locally and enterprise wide. In February 2011, we reported that CBP did not properly plan and implement the System Availability project, which was aimed at upgrading the local area networks at over 500 locations.[21] Specifically, it did not ensure that adequate funding was available, include all at-risk sites, or develop planning documents needed to justify project requirements and cost. Subsequently, CBP ran out of funding and ended the project in February 2010. As a result, hundreds of field sites did not receive the needed upgrades and remain vulnerable to network outages.

Additionally, in September 2011, we reported that the Department has made some progress toward consolidating the existing components' infrastructures into OneNet, the Department's wide area network initiative.[22] Specifically, it has established a centralized Network Operations Center/Security Operations Center incident response center and established a redundant network infrastructure and offers essential network services to its components. However, the Department still needs to establish component connections (peering) to OneNet and ensure that all components transition to the redundant trusted Internet connection.

Privacy

DHS continues to face challenges to ensure that uniform privacy procedures and controls are properly addressed and implemented throughout the lifecycle of each process, program, and information system that affects personally identified information (PII). In May 2011, we reported that USCIS demonstrated an organizational commitment to privacy compliance by appointing a privacy officer, establishing its Privacy Office, and making progress in implementing a privacy program that complies with privacy laws. However, we identified specific areas in privacy training, as well as technical and physical safeguards, to improve the protection of PII and the overall culture of privacy. [23]

---

[19] DHS-OIG, *U.S. Secret Service's Information Technology Modernization Effort (Redacted)* (OIG-11-56, March 2011).
[20] DHS-OIG, *Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology* (OIG-11-69, April 2011).
[21] DHS-OIG, *Planning and Funding Issues Hindered CBP's Implementation of the System Availability Project (Redacted)* (OIG-11-42, February 2011).
[22] DHS-OIG, *DHS Continues to Face Challenges in the Implementation of Its OneNet Project* (OIG-11-116, September 2011).
[23] DHS-OIG, *U.S. Citizenship and Immigration Services Privacy Stewardship* (OIG-11-85, May 2011).

EMERGENCY MANAGEMENT

Although FEMA has made great strides in improving its disaster preparedness and recovery, challenges remain, including in the areas of emergency support functions, mass care and debris removal.

Emergency Support Functions

The National Response Framework is a guide to how the Nation conducts all-hazards response. FEMA is the coordinator or primary agency for eight Emergency Support Functions and is responsible for ensuring that activities for these functions are accomplished as outlined in the National Response Framework. In November 2010, we released a report evaluating FEMA's readiness to fulfill its Emergency Support Function roles and responsibilities.[24] The review focused on three major areas of responsibility: (1) Coordination with Emergency Support Function Stakeholders, (2) Operational Readiness, and (3) Financial Management.

We found that FEMA generally fulfilled its roles and responsibilities under the Emergency Support Functions. Specifically, the agency manages mission assignments, executes contracts, and procures goods and services for its Emergency Support Function activities. We also concluded, however, that the agency can improve its coordination with stakeholders and its operational readiness. For example, FEMA should be coordinating with stakeholders for all Emergency Support Functions. There was little evidence that support agencies were regularly included in planning meetings for Emergency Support Function 3: Public Works and Engineering, even though agency officials said that such coordination would be beneficial. The agency must coordinate these activities with all relevant federal departments and agencies, state and local officials, and private sector entities to effectively execute the Emergency Support Function mission.

FEMA also should be fully prepared to provide community assistance after a disaster. At the time of our review, it was not conducting long-term recovery exercises, and one Emergency Support Function did not have clearly defined procedures to identify and deploy needed recovery services to disaster affected communities. FEMA did include a long-term recovery component in the National Level Exercise 2011. FEMA told us that since our report, they have increased engagement with Emergency Support Function partner agencies and have reinvigorated the Emergency Support Function Leadership Group.

Mass Care and Emergency Assistance

We evaluated FEMA's progress in two Emergency Support Function sections: mass care and emergency assistance.[25] Mass care includes sheltering, feeding, emergency first aid, distribution of emergency items, and collecting and providing information on victims to family members. Emergency assistance is the assistance necessary to ensure that immediate

[24] DHS-OIG, *Assessment of Federal Emergency Management Agency's Emergency Support Function Roles and Responsibilities*, (OIG-11-08, November 2010).
[25] DHS-OIG, *Opportunities to Improve FEMA's Mass Care and Emergency Assistance Activities*, (OIG-11-77, April 2011).

needs beyond the scope of the traditional mass care services are addressed. These services include evacuation support, aid and services to special needs populations, reunification of families, as well as a host of other evacuation, sheltering, and other emergency services, as well as coordination of voluntary agency assistance.

FEMA continues to improve its mass care and emergency assistance program. It has coordinated more effectively with state and local governments and voluntary organizations; developed planning tools to build the mass care and emergency assistance capacities of these governments and organizations; and created an internal infrastructure to plan, coordinate, and provide direct mass care and emergency assistance, as needed.

While FEMA has taken steps to improve, additional actions are needed to ensure that the program is implemented effectively in future disasters. Mass care and emergency assistance standard operating procedures are in draft form, years after being developed. The effectiveness of developed planning tools and initiatives have not always been evaluated. Mass care and emergency assistance activities have not always been included in national and regional exercises. In addition, an opportunity exists for improved efficiency by creating automated computer interfaces between FEMA and American Red Cross National Shelter System databases. Each of these databases track sheltering information needed during a disaster. At this time, these two databases do not interface.

Debris Removal Operations

FEMA's Public Assistance program has expended more than $8 billion over the past 11 years reimbursing applicants, primarily cities and counties, for removing debris resulting from natural disasters. In general this has been a successful effort; vast amounts of debris have been removed and disposed of, allowing communities to proceed with recovery efforts. Better planning, contracting, and oversight of debris removal operations, however, would enable these operations to be conducted in a more cost-effective manner.

Debris planning allows communities to be better prepared for a disaster by identifying debris collection and disposal sites, preparing debris removal contracts, and identifying potential debris contractors in advance of a disaster. Only a minority of states and local governments currently have such plans in place. A pilot program that operated in 2007–2008 was successful in encouraging the development of debris plans, but this momentum has been lost since the pilot program ended.

Decisions made in the first few days after a disaster strikes are critical in determining the success of a debris removal operation. Despite improved federal and state efforts to ensure that local governments are prepared for debris removal operations, they are often unprepared. FEMA debris advisers can help local governments determine what needs to be done, but qualified advisers are not always available when needed.

While FEMA has made significant strides in this area, opportunities remain for further improvement. Federal disaster response teams need to address debris expertise. Debris removal guidance is often unclear and ambiguous. Finally, an integrated performance

measurement system would provide federal and state officials and stakeholders with the data and tools to measure, analyze, and improve debris operations in a fact-based manner.

FEMA will be consolidating and updating the *Debris Monitoring Guide* and the *Debris Policy and Management Guide* into a single, comprehensive *Debris Policy and Management Guide* which will include detailed contracting guidance in FY 2012. FEMA will continue to make debris training available through the Emergency Management Institute, FEMA regional offices, and online. In addition, FEMA is currently developing a computer-based training course on debris management plan development that will be available to the public in FY 2012.

Since 2005, FEMA has worked to develop automated digital systems that will enhance FEMA's debris estimating and data collection capabilities in the field. FEMA is also developing a debris cost database to assist Public Assistance staff and applicants in determining whether a cost is reasonable. The debris cost database will also allow FEMA to analyze costs for debris operations across FEMA regions, disasters, states, and contractors. FEMA plans to implement these systems in FY 2012.

Fraud Prevention

Between January and September 2011, 10 separate billion dollar disasters have occurred in the United States.[26] The speed with which FEMA disburses individual and household disaster assistance results in the program's susceptibility to fraud. FEMA has established a Fraud Prevention and Investigation Branch to assist in the prevention and detection of fraud, but its operations are hindered by inadequate staffing and a lack of the latest technology tools to detect fraud. FEMA needs to improve its internal controls, provide fraud prevention training to all employees and support the Fraud Branch.[27]

[26] National Climate Data Center, http://www.ncdc.noaa.gov/oa/reports, accessed September 13, 2011.
[27] DHS-OIG, *Assessment of FEMA's Fraud Prevention Efforts*, (OIG-11-84, May 2011).

GRANTS MANAGEMENT

FEMA's grants management and oversight infrastructure is challenged by the need to improve monitoring of grantees.[28] FEMA has taken the following steps to improve grants management and its oversight infrastructure:

- Began a multi-year effort to improve programmatic and financial monitoring. The Programmatic Grants Monitoring Improvement Initiative will expand and enhance programmatic monitoring capacity, as well as form comprehensive plans for future grants monitoring. In conjunction with this initiative, FEMA has launched a web-based system for its non-disaster grants, called ND Grants, to consolidate the entire preparedness (non-disaster) grants management lifecycle into a single system. In addition, the initiative will transition monitoring data to a web-based environment that will allow for greater ease of use, more sophisticated analytics, and greater data coordination with other reporting efforts. To enhance financial monitoring, FEMA has refined criteria for deciding which grants to monitor, standardized Regional financial monitoring activities, and expanded ongoing oversight activities to ensure early identification of issues.

- Increased regional management of grant programs to improve customer service to grantees, increase grants administration efficiencies, and build more robust regions. A recent GAO review indicates that FEMA is making progress in managing regionalization of preparedness grants.

- Established performance measures for the FY 2011 Homeland Security Grant Program and the Emergency Management Performance Grant Program, and is n the process of creating metrics for the remaining preparedness grant programs. FEMA states that internal and external management and administrative performance measures are being developed to track how well grants are being managed. However, until FEMA finalizes these measures, we are unable to evaluate their effectiveness.

FEMA is taking steps to improve its grants policies, procedures, systems, and processes, which when developed and implemented, should strengthen its grants management and oversight infrastructure. The following highlights the agency's progress in two key areas: disaster and preparedness grants management.

Disaster Grants Management

While FEMA does not directly manage subgrants, it is incumbent on FEMA to make certain that States, as grantees, understand the rules and regulations that govern disaster grants and ensure that subgrantees adhere to these. We issued a report in August 2011 that recapped the reports we issued in FY 2010 and presented some of the most common findings that lead to questioned costs, including improper contracting practices, inadequate subgrantee contract monitoring, costs not adequately supported, and ineligible work and project charges. We

[28] *The Post Katrina Emergency Management Reform Act of 2006* centralized most of DHS' grant programs under FEMA's Grant Programs Directorate (GPD).

also reported five instances in which grantee management could be improved. Grantees: (1) did not have procedures in place to ensure that cash advances to subgrantees were expended timely and excess funds were recovered promptly, (2) did not have a documented or standard payment processing policy or needed to strengthen controls to prevent overpayments, (3) had no procedures in place to follow up on material deficiencies reported in Single Audits, (4) were unaware of significant budget and scope increases, or (5) did not adequately monitor and report subgrantee program performance.

In FY 2011, we issued 61 subgrant audit reports with nearly $308 million in questioned costs and over $23 million in funding that could be deobligated or collected and be put to better use.

Preparedness Grants Management

FEMA faces challenges in mitigating redundancy and duplication among preparedness grant programs, including barriers at the legislative, departmental, and state levels. The preparedness grant application process risks being ineffective because FEMA does not compare and coordinate grant applications across preparedness programs. Since grant programs may have overlapping goals or activities, FEMA risks funding potentially duplicative or redundant projects. We made recommendations designed to improve the management of these grant programs, with which FEMA agreed. In FY 2010, FEMA added Operation Stonegarden to the cluster of programs comprising the Homeland Security Grant Program. For FY 2011, activities previously included in the former Buffer Zone Protection Program and Interoperable Emergency Communications Program became eligible in the Homeland Security Grant Program.

FEMA should be able to accomplish our recommendations by addressing the specific grant-related recommendations of the October 2010 report of the congressionally mandated Local, State, Tribal and Federal Preparedness Task Force. However, until FEMA finalizes implementation plans with target dates for the Task Force recommendations, we cannot adequately evaluate the corrective actions to our recommendations.

Public Law 110-53, *Implementing Recommendations of the 9/11 Commission Act of 2007*, required the OIG to audit individual states' management of State Homeland Security Program and Urban Areas Security Initiatives grants and annually submit to Congress a report summarizing the results of these audits. In the audits we have completed to date, we have determined that the states have generally done an efficient and effective job of administering the grant management program requirements, distributing grant funds, and ensuring that all the available funds were used. We have identified several instances of states, as grantees, insufficiently monitoring subgrantee compliance with grant terms. Further, most states could not clearly document critical improvements in preparedness as a result of grant awards. In addition, we noted a need for improvement in the areas of timeliness of grant fund obligations and expenditures, compliance with procurement and inventory requirements, and identification of long-term capability sustainment options.

FINANCIAL MANAGEMENT

In FY 2010, the Department committed to obtaining a qualified opinion on the Balance Sheet and Statement of Custodial Activity. To that end, DHS continued to improve financial management in FY 2011 and has achieved a significant milestone. For FY 2011, DHS was able to produce an auditable balance sheet and statement of custodial activity; and the independent auditors rendered a qualified opinion on those financial statements. However, challenges remain. In order to sustain or improve its opinion, the Department must continue remediating the remaining control deficiencies. Additionally, in FY 2012 the auditors could identify additional control deficiencies in areas that had not been tested previously due to the increase in audit scope to all of the financial statements. Additional deficiencies could also cause the department to lose its opinion.

Although the Department continued to remediate material weaknesses and reduce the number of conditions contributing to the material weaknesses, five of the six material conditions from FY 2010 were repeated in FY 2011. DHS made some progress in two of the material weaknesses, and accordingly, those conditions were narrowed in scope. Specifically, DHS corrected the weakness conditions related to financial management, but not the deficiencies related to financial reporting; hence, financial management and reporting was reduced to financial reporting. Additionally, the auditors noted improvement in internal controls over Actuarial Liabilities, primarily because the Coast Guard was able to assert to over $40 billion of actuarial liabilities. The Coast Guard continues to have significant challenges in Environmental and Other Liabilities, which resulted in a material weakness for the Department during FY 2011. Further, as in previous years, the DHS Secretary has issued a statement of no assurance on the Department's internal controls over financial reporting, due to the existence of a pervasive material weakness, and limits on the scope of DHS' self assessment while focusing on remediation of control deficiencies. Consequently, the independent auditors were unable to render an opinion on DHS' internal controls over financial reporting in FY 2011.

During FY 2010, the independent auditors identified four department-wide control environment weaknesses that had a pervasive impact on the effectiveness of internal controls over consolidated financial reporting. In FY 2011, the independent auditors noted that only one of the four conditions still existed – the Department's financial information technology system infrastructure is aging and has limited functionally, which is hindering the Department's ability to implement efficient corrective actions and produce reliable financial statements. This issue is further discussed in the Information Technology Controls and Financial Systems Functionality section below.

The independent auditors noted that the DHS civilian components continued to make some progress in the remediation of IT findings that were reported in FY 2010. The Department closed approximately 31% of prior year IT findings. In FY 2011, the independent auditors issued approximately 135 findings, of which more than 65% are repeated from last year.

The remaining significant component-level challenges are primarily at the Coast Guard. In FY 2011, the Coast Guard made progress with implementing aspects of its *Financial Strategy for Transformation and Audit Readiness* (FSTAR) in the areas necessary to assert to

the auditability of its balance sheet, except for Property, Plant, & Equipment (PP&E), environmental liabilities, and related effects on other balance sheet line items. FSTAR calls for continued remediation of control deficiencies and reconciliation of balances in FY 2012.

Managerial Cost Accounting

The Department does not have the ability to provide timely cost information by major program, and strategic and performance goals as required by Office of Management and Budget Circular No. A-136, *Financial Reporting Requirements,* as amended. The Department does not have financial management systems that allow for the accumulation of costs, at the consolidated level, by major program, or allow for the accumulation of costs by responsibility segments that align directly with the major goals and outputs described in the entity's strategic and performance plans. Further, the Department has not developed a plan to implement managerial cost accounting, including necessary information systems functionality. Currently, the Department must use manual data calls to collect cost information from the various components and compile data on a consolidated basis.

The OIG conducted several audits during FY 2011 and found that a number of components did not have the ability to provide various cost data when requested. For example:

- In January 2011, we reported that CBP was unable to capture or track data related to the time officers and agents spend specifically on transportation and guard services for illegal aliens. Not having this data available prohibited CBP from having complete cost information to determine the most cost effective solution.[29] *U.S. Customs and Border Protection's Ground Transportation of Detainees*, OIG-11-27, January 2011.
- In March 2011, we issued a report on CBP's Efficacy of Controls Over Drug Seizures. During the course of the audit we learned that CBP was unable to estimate the cost of its drug seizure efforts.[30] *CBP's Efficacy of Controls Over Drug Seizures*, OIG-11-57, March 2011.
- In September 2011, we reported that the Coast Guard did not accurately capture and bill all indirect costs incurred for the Deepwater Horizon oil spill response effort. The results of the audit found that Coast Guard had adequate internal controls, policies, and procedures to accurately bill direct costs from the Deepwater Horicon oil spills, but the unprecedented size of the spill challenged its existing processes for capturing indirect costs and revealed weaknesses in these processes. The Coast Guard did not have adequate policies, procedures, and internal controls to ensure that indirect costs are verified using Coast Guard official systems of record.[31] *United States Coast Guard's Internal Controls and Cost Capturing for the Deepwater Horizon Oil Spill*, OIG-11-115, September 2011.

[29] DHS-OIG, *U.S. Customs and Border Protection's Ground Transportation of Detainees*, (OIG-11-27, January 2011).
[30] DHS-OIG, *CBP's Efficacy of Controls Over Drug Seizures*, (OIG-11-57, March 2011).
[31] DHS OIG, *United States Coast Guard's Internal Controls and Cost Capturing for the Deepwater Horizon Oil Spill*, (OIG-11-115, September 2011).

Anti-Deficiency Act Violations

The Department continues to have challenges with complying with the *Anti-Deficiency Act* (ADA). As of September 30, 2011, the Department reported six instances of potential ADA violations in various stages of review within the Department and its components. Management at the Coast Guard continues to work toward resolving four potential ADA violations, one of which was identified during FY 2011. Those potential ADAs relate to (1) funds may have been used in advance of an approved apportionment from OMB, (2) funds used for construction and improvement projects, (3) funds that were inappropriately used for modifications to fixed price contract, and (4) the improper execution of the obligation and disbursement of funds for the lease of passenger vehicles.

Financial Statements Audit

The following six items present the status of DHS' effort to address internal control weaknesses in financial reporting that were identified in FY 2010. Each item is divided into two categories: (1) Military – Coast Guard, and (2) Civilian – all other DHS components. These six items represent the six material weaknesses identified during the independent audit of the FY 2010 DHS consolidated balance sheet and statement of custodial activity. Five of the six weaknesses continued to exist throughout FY 2011 and were again noted in the FY 2011 Independent Auditors' Report. In FY 2011, the Fund Balance with Treasury material weakness was downgraded to a significant deficiency. Further, DHS made some progress in two of the material weaknesses, and accordingly, those conditions were narrowed in scope. Specifically, DHS corrected the weakness conditions related to financial management, but not the deficiencies related to financial reporting; hence, financial management and reporting was reduced to financial reporting. Additionally, the auditors noted improvement in internal controls over Actuarial Liabilities, primarily because Coast Guard was able to assert to over $40 billion of actuarial liabilities. Coast Guard continues to have significant challenges in Environmental and Other Liabilities, which resulted in a material weakness for the Department during FY 2011. For a complete description of the internal control weaknesses identified in the FY 2010 audit, see OIG-11-09.[32] To determine the status, we compared the material weaknesses reported by the independent auditor in FY 2010 with those identified in FY 2011.[33]

Based on the consolidated result of the six financial management areas included in the report, DHS has made measurable progress overall in financial management.

[32] DHS-OIG, *Independent Auditors' Report on DHS' FY 2010 Financial Statements and Internal Control over Financial Reporting*, (OIG-11-09, November 2010).
[33] DHS-OIG, *Independent Auditors' Report on DHS' FY 2011 Financial Statements and Internal Control Over Financial Reporting*, (OIG-12-07, November 2011).

Financial Reporting

Financial reporting is the process of presenting financial data about an agency's financial position, the agency's operating performance, and its flow of funds for an accounting period.

- Military:

  In previous years, the independent auditors noted that the Coast Guard had several internal control deficiencies that led to a material weakness in financial reporting. To address the material weakness conditions, the Coast Guard developed its *Financial Strategy for Transformation and Audit Readiness,* which is a comprehensive plan to identify and correct conditions that are causing control deficiencies. Significant control deficiencies contributing to a material weakness in financial reporting in FY 2010 included: (1) lack of sufficient financial management personnel to identify and address control weaknesses; and (2) lack of effective policies, procedures, and controls surrounding the financial reporting process.

  The Coast Guard has made progress in remediating the numerous internal control weaknesses identified by the independent auditor during FY 2010 in financial reporting. The Coast Guard implemented new policies and procedures, and automated tools to improve internal controls and the reliability of its financial statements. This effort has allowed the Coast Guard to assert to the auditability of all balance sheet accounts except property, plant and equipment and environmental liabilities. However, the Coast Guard does not have properly designed, implemented, and effective policies, procedures, processes, and controls surrounding its financial reporting process. Further, the FSTAR calls for continued remediation of control deficiencies and reconciliation of balances in FY 2012. Consequently, components of the financial reporting deficiencies reported in the past remain uncorrected at September 30, 2011.

- Civilian:

  In FY 2010, the independent auditors identified department-wide control weaknesses that have a pervasive effect on the effectiveness of internal controls over consolidated financial reporting. The auditors also found financial reporting internal control deficiencies at FEMA and TSA. Taken together, these deficiencies contributed to a departmental material weakness.

  During FY 2011, the Department made progress overall in addressing the department-wide control weaknesses over consolidated financial reporting. The independent auditors noted that during FY 2011, FEMA corrected control deficiencies that contributed to the overall material weakness. Although TSA continued to make progress by hiring property accounting personnel and completing reconciliation of its balance sheet accounts, it has not fully developed its financial reporting process with sufficient policies, procedures, and internal controls to ensure reliability of certain significant financial statement balances. Further, in FY 2011, control deficiencies at USCIS

contributed to the Department's material weakness in financial reporting. The auditors noted that in FY 2011, the Department implemented a change in accounting treatment of certain user fees collected by USCIS. The change resulted in the correction of an error in the presentation of user fees as reported in previous years, and identification of a control weakness in the financial reporting process. The auditors also noted that USCIS did not have sufficient policies and procedures or documentation supporting the process used to develop adjustments to deferred revenue. These combined internal control deficiencies contributed to the Department's financial reporting material weakness in FY 2011.

Information Technology Controls and Financial Systems Functionality

IT general and application controls are essential for achieving effective and reliable reporting of financial and performance data.

- Military:

  A number of the Coast Guard's challenges in financial reporting are due to the lack of an effective general ledger system. The Coast Guard currently uses multiple systems that do not comply with the requirements of the *Federal Financial Management Improvement Act.*

  In previous years the independent auditors noted that one of the most significant IT issues at the Coast Guard that could affect the reliability of the financial statements related to the development, implementation, and tracking of IT scripts, and the design and implementation of configuration management policies and procedures.

  During FY 2011, Coast Guard focused on improving documentation with the script change control process and implemented the final module of the script change management tool initiated in FY 2010. While the independent auditors noted that some previously identified control deficiencies were remediated, other deficiencies continued to exist. Coast Guard's core financial system configuration management process and financial system functionality remained a challenge to Coast Guard's ability to assert to all financial sheet balances during FY 2011. The auditors noted that the IT security access and configuration management controls were not operating effectively, and continued to present risks to DHS financial data confidentiality, integrity, and availability. Financial system functionality is inhibiting the Coast Guard's ability to implement and maintain internal controls supporting financial system data processing and reporting.

  The independent auditors also reported that financial data in the general ledger might be compromised by automated and manual changes that are not adequately controlled. The changes are implemented through the use of an IT scripting process, which was instituted as a solution to address functionality

and data quality issues. However, the controls over the script process were not properly designed or implemented effectively.

Financial systems functionality limitations are preventing the Coast Guard from establishing automated processes and application controls necessary to support accurate and reliable financial data. For example, existing limitations impair Coast Guard's ability to maintain adequate posting logic transaction codes to ensure that transactions are recorded in accordance with U.S. generally accepted accounting principles.

- Civilian:

  During FY 2010, the independent auditor identified IT control weaknesses in five areas that continued to present risks to the confidentiality, integrity, and availability of DHS' financial data: (1) access controls, (2) configuration management, (3) security management, (4) contingency planning, and (5) segregation of duties. Additionally, the independent auditors noted that in some cases financial system functionality inhibited DHS' ability to implement and maintain or install internal controls. These combined internal control deficiencies contributed to the Department's financial management and reporting material weakness in FY 2010.

  For FY 2011, DHS has made limited progress overall in correcting the IT general and applications control weaknesses identified in the FY 2010 Independent Auditors' Report. During FY 2011, DHS and its components corrected approximately 31% of the IT control weakness conditions that the auditors had identified in prior years. Coast Guard, FEMA, Federal Law Enforcement Training Center (FLETC), and ICE made the most progress in remediating the IT control weaknesses. Although conditions improved at Coast Guard, FEMA, FLETC, and ICE, conditions at CBP deteriorated during the year. The majority of new control deficiencies the independent auditors identified during the year were at CBP.

  The auditors noted that at the end of FY 2011, over 135 IT control weakness conditions existed, of which more than 65% are repeat from last year. Approximately 25% of the repeat findings were for IT deficiencies that management represented were corrected during FY 2011.

  The auditors noted that many of the financial systems in use at DHS components have been inherited from the legacy agencies and have not been substantially updated since DHS' inception. As a result, ongoing financial system functionality limitations are contributing to the Department's challenges in addressing systemic internal control weaknesses and strengthening the overall control environment.

  The FY 2011 Independent Auditors' Report noted that the IT control weaknesses remained for the five areas and continued to present risks to the

confidentiality, integrity, and availability of DHS' financial data: (1) access controls, (2) configuration management, (3) security management, (4) contingency planning, and (5) segregation of duties.

Property, Plant, and Equipment

DHS capital assets and supplies consist of items such as property, plant, and equipment, operating materials; and supplies, including boats and vessels at the Coast Guard, passenger and baggage screening equipment at TSA, and stockpiles of inventory to be used for disaster relief at FEMA.

- Military:

  The Coast Guard maintains approximately 49% of the Department's PP&E, including a large fleet of boats and vessels.

  For FY 2010, the independent auditors noted that the Coast Guard had difficulty establishing its opening PP&E balances primarily because of poorly designed policies, procedures, and processes implemented, combined with ineffective internal controls. PP&E was not properly tracked or accounted for many years preceding the Coast Guard's transfer to DHS in 2003. Furthermore, the fixed asset module of the Coast Guard's Core Accounting System (CAS) was not being updated timely for effective tracking and reporting of PP&E on an ongoing basis. As a result, the Coast Guard was unable to accurately account for its PP&E, and provide necessary information to DHS' Office of Financial Managment for consolidated financial statement purposes.

  In FY 2011, the Coast Guard continued to execute remediation efforts to address PP&E process and control deficiencies, specifically those deficiencies associated with vessels, small boats, aircraft, and select constuction in process projects. Remediation efforts are scheduled to occur over a multi-year timeframe beyond FY 2011. Consequently, the Coast Guard has made only limited progress in this area during FY 2011.

- Civilian:

  During FY 2010, CBP and TSA contributed to a departmental material weakness in PP&E. The deficiencies at TSA were more severe than at CBP.

  Although TSA made some progress in remediating control deficiencies during FY 2011, including having auditable beginning internal use software balance, it was unable to fully address all of the conditions that existed in FY 2010. Consequently, the overall severity of its internal control weakness conditions remained throughout FY 2011. Likewise, although CBP demonstrated some progress in remediating control deficiencies during FY 2011, the auditors identified control deficiencies similar to those noted in the prior year. Further,

internal control deficiencies were identified in the Office of Management that contributed to the overall DHS material weakness.

Environmental and Other Liabilities

Liabilities represent the probable and measurable future outflow or other sacrifice of resources as a result of past transactions or events. The internal control weaknesses reported in this area are related to various types of liabilities, including environmental, accounts payable, legal, and accrued payroll and benefits liabilities.

- Military:

  The Coast Guard's environmental liabilities consist of environmental remediation, clean up, and decommissioning, and represent approximately $973 million or 93% of total DHS environmental liabilities. Environmental liabilities are categorized as relating to shore facilities and vessels. Shore facilities include any facilities or property other than ships (e.g. buildings, fuel tanks, lighthouses, small arms firing ranges, etc).

  The independent auditors noted that during FY 2011, the Coast Guard continued to implement a multi-year remediation plan to address process and control deficiencies related to environmental liabilities. As a result, the Coast Guard made limited progress in implementing policies and procedures. However, most of the control weakness conditions reported in the FY 2010 Independent Auditors' Report remained throughout FY 2011.

- Civilian:

  No control deficiencies related to Environmental and Other Liabilities were identified at the civilian components in FY 2011.

Budgetary Accounting

Budgetary accounts are a category of general ledger accounts where transactions related to the receipt, obligation, and disbursement of appropriations and other authorities to obligate and spend agency resources are recorded.

- Military:

  The Coast Guard has over 80 Treasury Account Fund Symbol (TAFS) covering a broad spectrum of budget authority, including annual, multi-year, and no-year appropriations; and several revolving, special, and trust funds. Each TAFS with separate budgetary accounts must be maintained in accordance with OMB and Treasury guidance.

  Many of the conditions that contributed to a material weakness in budgetary accounting at the Coast Guard in FY 2010 remained throughout FY 2011. For example, the Coast Guard has not fully implemented policies, procedures, and internal controls over its process for validation and verification of undelivered order balances.

- Civilian:

  For FY 2010, internal control weaknesses at CBP and FEMA contributed to a material weakness in budgetary accounting for the Department.

  During FY 2011, the Department demonstrated moderate progress in correcting the budgetary accounting material weakness. The independent auditors noted that corrective actions CBP implemented during FY 2010 continued to be effective throughout FY 2011. Additionally, during FY 2011 FEMA continued to improve its processes and internal control over the obligation and monitoring process. However, some control deficiencies remained at FEMA. The control deficiencies at FEMA, combined with those at Coast Guard resulted in an overall material weakness in the area for the Department.

Fund Balance with Treasury

Fund Balance with Treasury (FBWT) represents accounts held at the Treasury from which an agency can make disbursements to pay for its operations. Regular reconciliation of an agency's FBWT records with Treasury is essential to monitoring and safeguarding these funds, improving the integrity of various U.S. Government financial reports, and providing a more accurate measurement of budget resources.

- Military:

  FBWT at the Coast Guard represents approximately 11% of total DHS FBWT. During FY 2010, the independent auditors reported a material weakness in internal control over FBWT at the Coast Guard. During FY 2011, the Coast Guard corrected several significant control deficiencies around FBWT. As a result, Coast Guard was able to assert to the completeness, existence, and accuracy of FBWT.

  However, the Coast Guard continues to have FBWT control deficiencies. For example, Coast Guard does not have a process in place to provide transaction-level supporting documentation for all reconciling items. Consequently, some of the weakness conditions that were reported in FY 2010 remain throughout FY 2011. The auditors consider the remaining weaknesses to be less severe, but still important enough to require management's attention.

- Civilian:

  No control deficiencies related to FBWT were identified at the civilian components in FY 2011. Corrective actions implemented in previous years continued to be effective throughout FY 2010 and FY 2011.

INFRASTRUCTURE PROTECTION

The need to rely on federal partners and the private sector to deter threats, mitigate vulnerabilities, and minimize incident consequences complicates protection efforts for all critical infrastructure and key resources and remains a great challenge for DHS.

Risk Assessment Efforts in the Dams Sector

Dams and related structures are especially important because one catastrophic failure at some locations could affect populations exceeding 100,000 and have economic consequences surpassing $10 billion. We reviewed the Department's risk assessments effort in the Dams Sector[34] to determine whether the Office of Infrastructure Protection has taken steps to assess risk at the most critical dam assets, and followed up to ensure that recommendations were implemented. We found the Department lacks assurance that risk assessments were conducted and security risks associated with critical dam assets were identified and mitigated. The Department did not: (1) review all critical dam asset risk assessments conducted by other agencies, (2) conduct security reviews for 55% of the critical dam assets, or (3) ensure that corrective actions were completed to mitigate risk when security gaps were identified.

DHS was unable to complete these tasks because it does not have the authority to ensure that security partners participate in risk management activities or that dam owners undergo departmental assessments and implement corrective action. The National Infrastructure Protection Plan prescribes a partnership approach between government and the private sector to voluntarily manage risk. Underlying legislation does not give the Department the necessary authority to ensure that security partners participate in risk management activities, or that dam owners undergo departmental assessments and implement corrective action. DHS could not always obtain cooperation from its security partners and dam owners and did not always collaborate successfully. This collaborative approach can be successful only if security partners and dam owners work together to perform risk management. The Assistant Secretary, Office of Infrastructure Protection, agreed with our recommendation to determine the appropriateness of a legislative proposal to establish regulatory authority for the critical Dams Sector assets similar to the Chemical Sector. Specifically, DHS personnel need authority to review risk assessments, conduct inspections when assessments are deficient, and make recommendations for corrective actions.

BORDER SECURITY

Securing the Nation's borders from the illegal entry of aliens, contraband, terrorists and weapons of mass destruction, while welcoming all legitimate travelers and trade, continues to be a major challenge. DHS apprehends hundreds of thousands of people and seizes volumes of illicit cargo entering the country each year. DHS is responsible for securing the 7,000 miles of international borders that the United States shares with Canada and Mexico.

[34] DHS-OIG, *DHS Risk Assessment Efforts in the Dams Sector*, (OIG-11-110, September 2011).

Western Hemisphere Travel Initiative

To address the challenge of facilitating the entrance of legitimate travelers while securing the Nation from illegal entry of aliens and terrorists, DHS and Department of State implemented the Western Hemisphere Travel Initiative (WHTI). WHTI requires citizens of the United States, Canada, Bermuda, and Mexico arriving at air, land and sea ports of entry to present passports or other approved documents to enter the United States. CBP is not prepared to fully enforce the new document requirement at land ports of entry. CBP has acquired and deployed substantial technological tools to aid in inspecting travelers arriving at land ports of entry. However, CBP has not analyzed the impact that a substantial increase in secondary inspection workload will have on secondary inspection staffing and infrastructure during full enforcement. The reported WHTI compliance rates during the initial eight-month informed compliance period indicate noncompliant travelers arriving at the agency's 39 busiest land ports may increase the secondary inspection workloads at these ports by an average of 73% if all noncompliant travelers required secondary inspections. Also, the agency has not finalized the operating procedures its officers will use to verify the identity and citizenship of noncompliant travelers.[35]

CBP's implementation of the WHTI document requirements have improved the agency's ability to validate the identity and citizenship of compliant air passengers, allowing officers to spend more time inspecting travelers without passports. However, there is inadequate assurance that CBP officers "verified" the identity and citizenship of all individuals who failed to provide a passport or other WHTI– compliant documentation. CBP officers did not always document the basis for their decisions to admit air passengers who were noncompliant with the new document requirements. Also, CBP officers did not always follow the agency's policy for referring all noncompliant passengers to a secondary inspection area for a more thorough review.[36]

Information Sharing on Foreign Nationals: Overseas Screening

DHS has implemented several programs to screen foreign nationals while they are still overseas. These programs rely on biographical, biometric, and documentary information in the Department's and other federal data systems. In our FY 2011 report, *Information Sharing on Foreign Nationals: Overseas Screening (Redacted)*,[37] we evaluated whether levels of cooperation, resources, and technology were adequate for Department officers to assess the risks posed by foreign nationals who seek to enter the United States. We also reviewed plans to consolidate and improve information in the Department's data systems. The Department has made progress in evaluating admissibility of foreign nationals before they travel to the United States. The level of cooperation among components that conduct overseas screening is high. Headquarters support offices have long-term plans to streamline

[35] DHS-OIG, *Customs and Border Protection's Implementation of the Western Hemisphere Travel Initiative at Land Ports of Entry*, (OIG-11-16, November 2010).
[36] DHS-OIG, *Customs and Border Protection Needs To Improve Its Inspection Procedures for the Western Hemisphere Travel Initiative* (OIG-11-43, February 2011).
[37] DHS-OIG, *Information Sharing On Foreign Nationals: Overseas Screening (Redacted),* (OIG-11-68, April 2011).

access to information in the Department's data systems, and improve screening and data analysis capabilities. However, DHS initiatives face serious resource and technological challenges. Information is fragmented among more than 17 data systems, and officers must conduct labor intensive, system-by-system checks to verify or eliminate each possible match to terrorist watch lists and other derogatory information.

CBP's National Targeting Center is challenged by insufficient staff and difficult working conditions. Effective small-scale screening and interdiction programs need sufficient resources to meet operational needs and congressional mandates. We made 18 recommendations to standardize the technology used to share information in Departmental data systems, enable federal officers to obtain and use the most current and complete data available, and improve information sharing procedures. Departmental components concurred with 17 of the 18 recommendations. However, for five recommendations with which components concurred, including three that would increase productivity for thousands of DHS employees, components said that they would need to request additional resources in the next federal budget cycle to implement the recommendations.

TRANSPORTATION SECURITY

TSA is responsible for protecting the transportation system and ensuring the freedom of movement for people and commerce. The Nation's economy depends upon secure, yet efficient transportation security measures. Although TSA is making progress, it continues to face challenges with strengthening security for aviation, mass transit and other modes of transportation.

Passenger and Baggage Screening

TSA's screening of persons and property continues to be a vital element of the overall aviation security system. The *Aviation and Transportation Security Act*[38] requires TSA to prescribe requirements for screening or inspecting all passengers, goods, and property before entry into the sterile areas of an airport. Our covert testing of carry-on baggage screener performance revealed that improvements are needed in the screening process to ensure that dangerous prohibited items are not cleared for loading onto a passenger aircraft.[39] The same report identified needed improvements for TSA's Advanced Imaging Technology.

Airport Badging Process Oversight

TSA's responsibilities include ensuring that employees working in secured airport areas are properly vetted and badged. The agency relies on designated airport operator employees to perform the badging application process. We reported that individuals who pose a threat may obtain airport badges and gain access to secured airport areas.[40] We analyzed vetting

[38] Public Law 107-71, November 19, 2001.
[39] DHS-OIG, *Evaluation of Newly Deployed and Enhanced Technology and Practices at the Passenger Screening Checkpoint (Unclassified Summary)* (OIG-10-75, March 2010).
[40] DHS-OIG, *TSA's Oversight of the Airport Badging Process Needs Improvement (Redacted)* (OIG-11-95, July 2011).

data from airport badging offices and identified badge holder records with omissions or inaccuracies pertaining to security threat assessment status, birthdates, and birthplaces.

These problems exist because TSA has designed and implemented only limited oversight of the application process. Specifically, the agency did not (1) ensure that airport operators have quality assurance procedures for the badging application process; (2) ensure that airport operators provide training and tools to designated badge office employees; and (3) require its Transportation Security Inspectors to verify the airport data during their reviews.

Passenger Air Cargo Security

Approximately 7.6 million pounds of cargo are transported on passenger planes each day. Federal regulations (49 CFR) require that, with limited exceptions, passenger aircraft may only transport cargo originating from a shipper that is verifiably "known" either to the aircraft operator or to the indirect air carrier that has tendered the cargo to the aircraft operator. Through covert testing, we identified vulnerabilities in the cargo screening procedures employed by air carriers and cargo screening facilities to detect and prevent explosives from being shipped in air cargo transported on passenger aircraft.[41] Although TSA has taken steps to address air cargo security vulnerabilities, our undercover audit demonstrated that the agency does not have assurance that cargo screening methods always detect and prevent explosives from being shipped in air cargo transported on passenger aircraft.

Training

Transportation Security Officers screen passengers, carry-on baggage, and checked baggage to prevent prohibited objects from being transported on aircraft. TSA can improve its management of the training program for the screening workforce.[42] The agency needs to develop and document standard processes to (1) use officer test results to evaluate training program results; (2) assign on-the-job training responsibilities; and (3) evaluate workforce and training needs to ensure that officers have the tools and time necessary to complete training requirements.

TSA did not establish a lead office to organize and coordinate Transportation Security Officer training until 2006. The agency issued a management directive designating the Operational and Technical Training Division responsible for the overall management of the analysis, design, development, and implementation of Transportation Security Officer training programs. However, the division did not assume an active leadership role until 2009 due to its need to maintain current training levels and respond to emerging threats. Without a documented process for updating training based on screener performance data and changes in technology or equipment, the TSA may be missing opportunities to enhance its officers' skills and abilities.

---

[41] DHS-OIG, *Evaluation of Screening of Air Cargo Transported on Passenger Aircraft,* (OIG-10-119, September 2010).

[42] DHS OIG, *Transportation Security Administration's Management of Its Screening Workforce Training Program Can Be Improved* (OIG-11-05, October 2010).

Rail and Mass Transit

Passenger rail stations are attractive terrorist targets because of the large number of people in a concentrated area. Amtrak provides passenger rail service for about 27 million passengers every year, using approximately 22,000 miles of rail in 46 states and the District of Columbia. We identified that grant recipients, such as Amtrak, transit agencies, and state and local authorities, coordinate risk mitigation projects at high-risk rail stations. However, Amtrak is not always using grant funds to implement mitigation strategies at the highest risk rail stations, in terms of casualties and economic impact.[43] Amtrak has not mitigated critical vulnerabilities reported in risk assessments. These vulnerabilities remain because TSA (1) did not require Amtrak to develop a corrective action plan addressing its highest ranked vulnerabilities; (2) approved Amtrak investment justifications for lower risk vulnerabilities; and (3) did not document roles and responsibilities for the grant award process.

The Transportation Sector Network Management, Mass Transit and Passenger Rail Division, needs to work closely with Amtrak to establish a corrective action plan that ensures decisions to fund Amtrak rail station remediation projects focus on mitigating the highest vulnerabilities identified by previous risk assessments. The Transportation Sector Network Management, Mass Transit and Passenger Rail Division needs to create and report internal procedures that describe how the agency will carry out its roles and responsibilities in the grant award process for ensuring that Amtrak and other grant recipients address the highest priority security vulnerabilities.

TRADE OPERATIONS AND SECURITY

CBP is charged with the dual mission of securing the Nation's borders, while facilitating legitimate trade and travel. While CBP continues to take action in this area, challenges remain with strengthening internal controls over revenue and protecting our Nation from security threats.

Customs Revenue

Customs revenue remains the second largest source of revenue for the U.S. government. CBP collected an estimated $32 billion in duties, fees, and taxes (revenue) in FY 2010, an increase of 9.5% over FY 2009. In the current economic environment, it is imperative CBP ensure that participating importers comply with federal trade requirements and that government revenues are protected. In 2010 and 2011, OIG conducted revenue audits of the Importer Self Assessment program[44] and the Single Transaction Bonds process[45] and found significant issues remain with oversight of these programs. The Importer Self Assessment program was initiated in 2002 as a voluntary approach to trade compliance. It is based on the

[43] DHS-OIG, *DHS Grants Used for Mitigating Risks to Amtrak Rail Stations (Redacted)* (OIG-11-93, June 2011).
[44] DHS-OIG, *Customs and Border Protection's Importer Self-Assessment Program*, (OIG-10-113, August 2010).
[45] DHS-OIG, *Information Technology Management Letter for the Federal Emergency Management Agency Component for the FY 2009 DHS Integrated Audit,* (OIG-10-92, May 2010).

premise that importers with strong internal controls achieve the highest level of compliance with federal trade laws and regulations and require less enforcement review and oversight. Our most recent review highlighted several areas where improvement can be made, including establishing and enforcing policies and procedures to document management controls and assessing risks to trade compliance.

Further, we noted that CBP needs to improve internal controls over the Single Transaction Bonds process which protects CBP from revenue loss when importers fail to fulfill their financial obligations. In 2011, the OIG conducted an audit of CBP's Single Transaction Bond program and found that from FY 2007 through FY 2010, CBP lost $46.3 million in revenue because of inaccurate, incomplete, or missing bonds. We recommended that CBP develop a risk based approach that includes identification, assessment, and mitigation of the risk of revenue loss associated with the single transaction bonding process.

Cargo Security

Ensuring that only legitimate cargo is allowed entry into the United States while facilitating the free flow of trade remains a challenge. Based on our FY 2010 audits, *CBP's Cargo Targeting and Examinations*[46] and *CBP's Ability to Detect Biological and Chemical Threats in Maritime Cargo Containers*,[47] we concluded that targeting and examination of high risk shipments continues to be a challenge for CBP. For example, CBP needs to update its guidance relating to the physical examinations of high-risk cargo containers that may contain biological, chemical, nuclear, and radiological threats and conduct a risk assessment to determine which pathways pose the highest risk.

The Free and Secure Trade (FAST) program is a commercial clearance program for known low-risk shipments entering the United States from Canada and Mexico. FAST allows for expedited processing of entities that have completed background checks and fulfill certain eligibility requirements. Improvements are needed in CBP's initial enrollment process for carriers to ensure that only low-risk carriers are allowed to participate in the FAST program. Highway carriers that did not meet all Custom-Trade Partnership against Terrorism's minimum security requirements have been certified to receive FAST program benefits. Also, the CBP Vetting Center and Trade Partnership against Terrorism supply chain security specialists did not always follow established procedures when determining the initial eligibility of highway carriers.[48]

Developing and maintaining a multi-layered risk based approach to trade security is a significant challenge. Section 1701 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* requires DHS to screen all cargo destined for the U.S. that is loaded on or after July 1, 2012. Over the past two years, CBP and DHS have raised concerns to Congress about the feasibility of 100% screening and have advocated for continuing to use a

[46] DHS-OIG, *Cargo Targeting and Examinations,* (OIG-10-34, January 2010).
[47] DHS-OIG, *CBP's Ability to Detect Biological and Chemical Threats in Maritime Cargo Containers,* (OIG-10-01, October 2009).
[48] DHS-OIG, *Improvements Needed in the Process to Certify Carriers for the Free and Secure Trade Program* (OIG-11-25, March 2011).

risk-based approach to meet the intent of mitigating high risk cargo. Regardless of whether DHS formally adopts 100% screening or continues to use its risk-based approach to trade security, DHS must ensure that it has adequate resources, infrastructure, and processes. DHS must also be able to reach agreement with the international community to resolve issues concerning corresponding resources, oversight, costs, timing, and enforcement considerations, as well as a process to resolve disagreements as they arise.

Appendix A
Management Comments to the Draft Report

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

Homeland Security

October 31, 2011

Charles K. Edwards
Acting Inspector General
Office of Inspector General
U.S. Department of Homeland Security
245 Murray Lane, SW, Building 410
Washington, DC 20528-0305

Re: Draft Report OIG Project No. 11-150-AUD-NONE, "Major Management Challenges Facing the Department of Homeland Security"

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 the DHS Office of Inspector General's (OIG's) work in planning and conducting its review and issuing this report in conjunction with the Department's FY 2011 Annual Financial Review. The Department concurs with the OIG's assessment that

> …the Department has made progress in coalescing into an effective organization, as well as addressing its key mission areas to secure our nation's borders, increase our readiness and resiliency in the face of a terrorist threat or a natural disaster, and implement increased levels of security in our transportation systems and trade operations.

DHS and its many partners across the Federal Government, public and private sectors, and communities across the country and around the world have worked to build a new homeland security enterprise to better mitigate and defend against dynamic threats, minimize risks, and maximize the ability to respond to and recover from attacks and disasters of all kinds while maturing and strengthening the Department's management functions.

In February 2010, DHS issued its first Quadrennial Homeland Security Review (QHSR) report, outlining a strategic framework for homeland security to guide the activities of the Department and its homeland security partners, including federal, state, local, and tribal government agencies; the private sector; and nongovernmental organizations and representing the most comprehensive assessment and analysis of homeland security to date.[1] The report identified five homeland security missions—Preventing Terrorism and Enhancing Security; Securing and Managing Our Borders; Enforcing and Administering Our Immigration Laws; Safeguarding and Securing Cyberspace; and Ensuring Resilience to Disasters—and goals and

[1] DHS, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (Washington, D.C.: February 2010).

1

objectives to be achieved within each mission. The report also identifies goals and objectives for maturing and strengthening the homeland security enterprise.

This first QHSR report has set the stage for detailed analyses of homeland security capabilities and requirements. This report will drive Department progress by redefining the homeland security missions and setting prioritized goals, objectives, and strategic outcome statements for each mission, and guiding all homeland security stakeholders toward common goals and objectives. A coordinated approach that promotes unity of effort will provide the foundation to combat current, emerging, and future threats to the homeland.

In each of the areas identified in the QHSR, we have continued to grow and mature as a Department by strengthening our existing capabilities, building new ones where necessary, enhancing our partnerships across all levels of government and with the private sector, and streamlining our operations and increasing efficiency.

Eight years since the Department's creation, and 10 years after the September 11, 2001 terrorist attacks, the results are clear: we have created a more effective and integrated Department, a strengthened homeland security enterprise, and a more secure America that is better equipped to confront the range of threats we face.

Again, thank you for the opportunity to review and comment on this draft report. We appreciate the OIG's continued work to assist in identifying management challenges that remain while recognizing the significant progress the Department has made over the past 8 years. This report and the Department's detailed response will be included in the Department's FY 2011 Annual Financial Report, as required by law. Technical and sensitivity comments have been provided under separate cover.

Sincerely,

Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

2

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
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 Management
Chief Financial Officer
Chief Information Officer
Chief Security Officer
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202)254-4100, fax your request to (202)254-4305, e-mail your request to our OIG Office of Public Affairs at DHS-OIG.OfficePublicAffairs@dhs.gov, or visit our OIG websites at www.dhs.gov/oig or www.oig.dhs.gov.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to Department of Homeland Security programs and operations:

- Call our Hotline at 1-800-323-8603
- Fax the complaint directly to us at (202)254-4292
- E-mail us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigation - Hotline,
  245 Murray Drive SW, Building 410
  Washington, DC 20528

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