



Department of Homeland Security Office of Inspector General

Major Management Challenges Facing the Department of Homeland Security



OIG-11-11

November 2010



Homeland
Security

November 10, 2010

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 FY 2010 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.

A handwritten signature in cursive script that reads "Richard L. Skinner".

Richard L. Skinner
Inspector General



Homeland
Security

Major Management Challenges Facing the Department of Homeland Security

In the aftermath of the terrorist attacks against America on September 11th, 2001, the Department of Homeland Security (DHS) was formed from 22 disparate domestic agencies. The creation of DHS represented one of the largest and most complex restructurings in the federal government. The Department of Homeland Security performs a broad range of activities across a single driving mission to secure America from the entire range of threats that we face.

Since its inception, the department has taken aggressive measures to secure our nation's borders, reform our nation's immigration laws, and take on the shared responsibility to make our country more ready and resilient in the face of a terrorist threat or a natural disaster. Although the department has taken steps to become "One DHS"; much remains to be done to establish a cohesive, efficient, and effective organization.

The major management challenges we identify facing DHS, including department-wide and operational challenges, are a major factor in setting our priorities for audits, inspections, and evaluations of DHS' programs and operations. As required by the *Reports Consolidation Act of 2000*, Pub.L.No. 106-531, we update our assessment of management challenges annually. We have made recommendations in many, but not all, of these areas as a result of our reviews and audits of departmental operations. Where applicable, we have footnoted specific reports that require DHS' action.

We have identified the following major management challenges:

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

Since the major management challenges have tended to remain the same from year to year, we developed scorecards to distinguish the department’s progress in selected areas. This report features scorecards for acquisition management, information technology management, emergency management, grants management, and financial management.

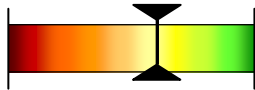
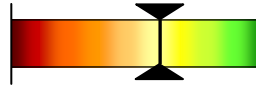

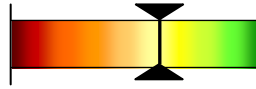
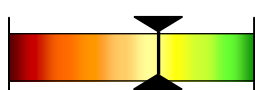
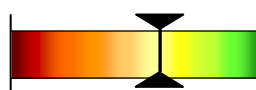
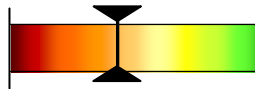
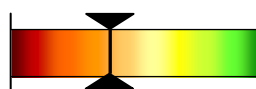
We based the ratings on a four-tiered scale ranging from limited to substantial progress:



- **Limited:** While there may be plans to address critical success factors, few if any have been implemented;
- **Modest:** While some improvements have been made, many of the critical success factors have not yet been achieved;
- **Moderate:** Many of the critical success factors have been achieved; and
- **Substantial:** Most or all of the critical success factors have been achieved.

These five scorecards are summarized in Figure 1 and incorporated in our discussion of the major management challenges.

Figure 1.

| | FY 2009 | FY 2010 |
|--|---|--|
| Acquisition Management | Moderate Progress  | Moderate Progress  |
| Information Technology Management | Moderate Progress  | Moderate Progress  |
| Emergency Management | Moderate Progress  | Moderate Progress  |
| Grants Management | Modest Progress  | Modest Progress  |

| | FY 2009 | FY 2010 |
|-----------------------------|-------------------------------|-------------------------------|
| Financial Management | <p>Modest Progress</p> | <p>Modest Progress</p> |

ACQUISITION MANAGEMENT

DHS relies on contractor support to fulfill its critical mission needs. An effective acquisition management infrastructure is vital to achieve DHS’ overall mission. It requires a sound management infrastructure to oversee the complex and large dollar procurements. It must identify mission needs; develop strategies to fulfill those needs while balancing cost, schedule, and performance; and ensure that contract terms are satisfactorily met.

A successful acquisition process depends on the following key factors:

- **Organizational Alignment and Leadership**—ensures appropriate placement of the acquisition function, defines and integrates roles and responsibilities, and maintains clear, strong executive leadership;
- **Policies and Processes**—partnering with internal organizations, effective use of project management approaches, and establishment of effective internal controls;
- **Acquisition Workforce**—commitment to human capital management, integration and alignment of human capital approaches with organizational goals, and investment in people; and
- **Knowledge Management and Information Systems**—tracking of key acquisition data, analysis of supplies and services spending, and data stewardship.

Acquisition Management Scorecard

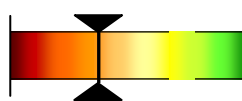
The following scorecard illustrates areas where DHS improved its acquisition management practices, as well as areas where it continues to face challenges. We based our assessment on our recent audit reports, GAO reports, congressional testimony, and our broader knowledge of the acquisition function.

Based on the consolidated result of the four acquisition management capability areas, DHS made “**moderate**” overall progress in the area of Acquisition Management.

ACQUISITION MANAGEMENT SCORECARD

Organizational Alignment and Leadership

Modest Progress



In both FY 2010 and FY 2009 DHS made “modest” progress in improving the acquisition program’s organizational alignment and defining roles and responsibilities. This rating remains unchanged because the department continues to depend on a system of dual accountability and collaboration between the chief procurement officer and the component heads, which may sometimes create ambiguity about who is accountable for acquisition decisions. However, DHS maintains that the dual authority model works because the Office of the Chief Procurement Officer (OCPO) retains central authority over all contracting through its contracting officer warrant program and Federal Acquisition Certification - Contracting program. According to the department, the heads of contracting activities and contracting officers function independently of component influence as their authority flows from OCPO rather than the component. DHS’ Acquisition Line of Business Integration and Management Directive sets forth existing authorities and relationships within individual components and the department’s Chief Procurement Officer.

According to the GAO)¹ DHS has not effectively implemented or adhered to its investment review process, which requires executive decision making at key points in an investment’s life cycle. In January of this year, the department published Acquisition Management Directive 102-01. The directive provides policy guidance to identify and track new and ongoing major investments and involves senior management in the investment review process by way of departmental oversight board reviews.

The department’s OCPO has made progress in its efforts to improve oversight of contracting activities by conducting reviews and issuing memoranda to component Heads of Contracting Activities (HCA). Specifically, between June 2007 and June 2010, OCPO conducted baseline oversight reviews of component procurement activities and provided each of the eight component HCAs with a report containing recommendations specific to their components. These reviews measured component compliance with applicable Federal regulations, departmental regulations, departmental acquisition manuals, policies, and guidance, and also established a baseline of issues and concerns for future on-site reviews. The reviews focused on major areas consistent with the framework for previously identified management challenges, such as organizational alignment, procurement management, human capital, knowledge and information management, and financial accountability.

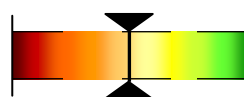
¹ GAO-09-29, *Department of Homeland Security: Billions Invested in Major Programs Lack Appropriate Oversight*, November 2008.

ACQUISITION MANAGEMENT SCORECARD

Additionally, on March 2, 2010, OCPO issued a special review of contracts awarded noncompetitively.² This report contained recommendations to HCAs for opportunities to improve the availability and accessibility of contract files; accurately code contract file information in the Federal Procurement Data System (FPDS); properly cite the authority to award a contract noncompetitively; and ensure that adequate rationale exists to support justifications and approvals.

Policies and Processes

Moderate Progress



DHS made “moderate” progress in developing and strengthening acquisition management policies and processes. For example, OCPO has updated the Homeland Security Acquisition Manual (HSAM) to improve the level of guidance provided to component HCAs. OCPO issued revisions to the HSAM that included a guide to components in conducting market research.³ Additionally, OCPO plans to amend the HSAM to require that acquisition personnel include Advanced Acquisition Plan numbers in procurement files, when applicable.⁴ The department also effectively conveyed critical information through the issuance of acquisition alerts to HCAs. During this fiscal year, OCPO distributed a DHS acquisition alert containing critical changes in reporting requirements for specific data elements in FPDS and another acquisition alert to familiarize HCAs with changes to competition information in FPDS.⁵ Although the department has taken steps towards improving its processes and controls over awarding, managing, and monitoring contract funds, we continue to identify problems in the acquisition area.

² DHS-OCPO, *CPO Special Procurement Oversight Review of Noncompetitive Contracts* (Report No. 10-001-S, March 2, 2010).

³ DHS-Homeland Security Acquisition Manual, Revisions to HSAM Chapters 3003, 3005, 3009, and Related Appendices (HSAM Notice 2010-02, December 16, 2009).

⁴ DHS-OIG, *DHS Contracts Awarded Through Other Than Full and Open Competition During Fiscal Year 2009* (OIG-10-55, February 2010).

⁵ DHS-OCPO, *Version 1.4 Changes in the Federal Procurement Data System Next Generation* (DHS Acquisition Alert 10/09, Amendment 1, March 25, 2010); DHS-OCPO, *Changes to Reporting of Competition Information in the Federal Procurement Data System-Next Generation*, October 29, 2009.

⁶ An award fee is an amount of money that a contractor may earn in whole or in part by meeting or exceeding subjective criteria stated in an award fee plan.

⁷ DHS-OIG, *Internal Controls in the FEMA Disaster Acquisition Process*, (OIG-09-32, February 2009); DHS-OIG, *Challenges Facing FEMA's Disaster Contract Management*, (OIG-09-70, May 2009); DHS-OIG, *FEMA's Acquisition of Two Warehouses to Support Hurricane Katrina Response Operations*, (OIG-09-77, June 2009); DHS-OIG, *FEMA's Temporary Housing Unit Program and Storage Site Management*, (OIG-09-85, June 2009).

⁸ GAO-09-630, *Federal Contracting: Guidance on Award Fees Has Led to Better Practices but is Not Consistently Applied*, May 2009.

ACQUISITION MANAGEMENT SCORECARD

As reported last year, DHS has not developed methods for evaluating the effectiveness of an award fee⁶ as a tool for improving contractor performance, and Federal Emergency Management Agency (FEMA) needs to accelerate its planned acquisition process improvements for awarding, managing, monitoring, tracking, and closing-out contracts.⁷ In May 2009, GAO⁸ reported that DHS provided guidance on award fees in its acquisition manual, but individual contracting offices developed their own approaches to executing award fee contracts that were not always consistent with the principles in the Office of Management and Budget’s guidance on award fees or among offices within DHS.

Acquisition Workforce

Moderate Progress



Although DHS made “moderate” progress in recruiting and retaining a workforce capable of managing a complex acquisition program, it continues to face workforce challenges across the department. A January 2010 report by the GAO indicated that as of April 2010, the Coast Guard filled 760 of its 951 military and civilian personnel positions in its acquisition branch.⁹ The Coast Guard received 100 additional acquisition positions for FY10 and intends to allocate twenty-five percent of these positions to the Offshore Patrol Cutter acquisition program. The Coast Guard is using contractors to fill its acquisition personnel gap and according to GAO, the Coast Guard is mitigating the potential for conflicts of interest and support of inherently governmental functions by releasing guidance to define inherently governmental roles and the role of Coast Guard personnel in contractor oversight.

FEMA has improved acquisition training and greatly increased the number of acquisition staff, but needs to better prepare its acquisition workforce for catastrophic disasters.¹⁰ Further, although FEMA continues to receive additional authorized acquisition staff positions, it has difficulty filling the positions due to the limited number of people with the needed skill set and the fierce competition across federal agencies for skilled acquisition personnel.

Over the past few years, DHS has centralized recruitment and hiring of acquisition personnel, established the Acquisition Professional Career Program to hire and mentor procurement interns, created a tuition assistance program, and structured rotational and development work assignments.¹¹ Although these are very positive steps, it will, in all likelihood, take years before the department has a fully staffed and fully skilled acquisition workforce.

⁹ GAO-10-268R, *Coast Guard: Service Has Taken Steps to Address historic Personnel Problems, but It is too Soon to Assess the Impact of These Efforts*, January 2010.

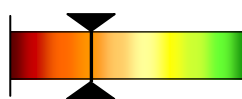
¹⁰ DHS-OIG, *Challenges Facing FEMA's Acquisition Workforce*, (OIG-09-11, November 2008).

¹¹ *Department of Homeland Security FY 2008 Annual Financial Report*.

ACQUISITION MANAGEMENT SCORECARD

Knowledge Management and Information Systems

Modest Progress



DHS has made “modest” progress in deploying an enterprise acquisition information system and tracking key acquisition data, however it has not fully deployed a department-wide (enterprise) contract management system that interfaces with the financial system. Many procurement offices continue to operate using legacy systems that do not interface with financial systems. With ten procurement offices and more than \$17 billion in annual acquisitions and procurement, DHS needs a consolidated acquisition system to improve data integrity, reporting, performance measurement, and financial accountability.

DHS needs to strengthen its controls for developing and implementing its systems consolidation project. The DHS Chief Financial Officer has initiated the Transformation and Systems Consolidation project to acquire an integrated financial, acquisition, and asset management solution for DHS. However, we reported in July 2010 that this project faces challenges because DHS does not have the necessary planning documents in place and approval for this effort; total life cycle cost estimates are not inclusive of all project costs; and staffing projections have not been finalized.¹² Additionally, DHS’ Office of Chief Information Officer has had limited involvement with the overall initiative, which increases the risk that the DHS Enterprise Architecture and security requirements may not be incorporated into the new system.

The department has made moderate progress to improve the accuracy and completeness of contract data in FPDS-NG.¹³ This system is the only consolidated information source for analyzing competition on procurements and is relied on for reporting to the public and Congress. This year, we reviewed the integrity of reported acquisition data in FPDS-NG and found that, although errors were detected in the data we sampled, the system earned a 94.5 % accuracy rate.¹⁴

Additional initiatives the department reports as being underway in the acquisition area include piloting the Procurement Enterprise Reporting Application (ERA) that will provide near real-time access to procurement data allowing for the consolidation, analysis, and review of the data from the disparate contract writing systems that will interface with the Federal Procurement Data System-Next Generation (FPDS-NG). User acceptance and data validation exercises are scheduled for October 2010 and the system is expected to be fully operational by January 2011. Also, OCPO outlined additional

¹² DHS-OIG, *DHS Needs to Address Challenges to Its Financial Systems Consolidation Initiative*, (OIG-10-95, July 2010)

¹³ DHS-OIG, *DHS Contracts Awarded Through Other Than Full and Open Competition during Fiscal Year 2007*, (OIG-09-94, August 2009).

¹⁴ DHS-OIG, *Department of Homeland Security’s Acquisition Data Management Systems*, (OIG-10-42, January 2010).

ACQUISITION MANAGEMENT SCORECARD

steps to ensure continued improvement in data accuracy that include developing training focused on preventing errors, increasing participation in the DHS FPDS working group aimed at improving the accuracy of data input in FPDS, and distributing 56 “data flags” to alert HCAs in identifying and correcting errors in FPDS data.

INFORMATION TECHNOLOGY MANAGEMENT

Creating a unified information technology infrastructure for effective integration and agency-wide management of 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.

Security of IT Infrastructure.

During our FY 2008 *Federal Information Security Management Act*¹⁵ (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 weaknesses remediation, quality of certification and accreditation, annual testing and validation, and security program oversight. The department also finalized its Sensitive Compartmented Information Systems Information Assurance Handbook, which provides department intelligence personnel with security procedures and requirements to administer its intelligence systems and the information processed.

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.

In July 2010 we reported that 5 components maintained 11 external network connections to other agency’s human resources systems that are outside of the DHS trusted internet connections (TIC)¹⁶. When components are allowed to maintain their own network connections to other federal agencies it increases the number of internet points of presence. This is contradictory to Office of Management and Budget’s TIC and DHS OneNet initiatives to improve efficiency and security by reducing the internet points of presence and may pose a security risk to DHS’ data if security controls implemented are inadequate.

¹⁵ Title III of the E-Government Act of 2002, Public Law 107-347.

¹⁶ DHS-OIG, *Management Oversight and Component Participation Are Necessary to Complete DHS’ Human Resource Systems Consolidation Effort*, (OIG-10-99, July 2010)

IT Management

Some DHS components face challenges when planning for and managing information technology to support DHS' mission. For example, Immigrations and Customs Enforcement (ICE) implemented an Office of the Chief Information Officer (OCIO) organizational strategic plan but did not define key goals and objectives for fulfilling its mission responsibilities. The ICE OCIO also has oversight of information technology spending, but its budget planning process did not capture all component information technology needs. In addition, we reported in July 2010 that DHS has made progress in consolidating its human resource systems.¹⁷ However, DHS faces additional challenges with implementing all of the enterprise-wide human resource solutions because many of the components are reluctant to adopt the department's enterprise-wide solutions.

Staffing shortages have also made it difficult for some DHS component CIOs to provide effective IT planning and management oversight. For example, ICE did not have the requisite staff to finalize its IT Strategic Plan. As a result ICE was not able to communicate its IT strategic goals and objectives to its stakeholders, create a formal process to facilitate IT policy development, approval, and dissemination, or establish an agency-wide IT budget process to include all ICE component office technology initiatives and requirements. In addition, the U.S. Citizenship and Immigration Services (USCIS) OCIO found it difficult to update its IT transformation approach, strategy, or plan. Without the necessary staff, USCIS OCIO was unable to document the results and lessons learned from the pilot and proof-of-concept programs that support its IT transformation program.

The department faces significant challenges as it attempts to create a unified IT infrastructure for effective integration and agency-wide management of IT assets and programs. To address these challenges, DHS has several initiatives underway to improve IT operations and reduce costs. One such program is to develop an enterprise-wide IT disaster recovery program to ensure that the department's operations can continue uninterrupted should its IT systems fail. A second related program is DHS' effort to consolidate its various data centers into two enterprise data centers. We reported in April 2009 that DHS had made progress in these two areas by allocating funds to establish the new data centers.¹⁸ However, we noted that more work was needed to ensure the new data centers were fully capable of meeting the department's significant IT disaster recovery needs. We also reported in September 2010, the DHS should undertake additional steps to successfully migrate its systems to these enterprise data centers.¹⁹

Privacy

DHS continues to face challenges to ensure that uniform privacy procedures and controls are properly addressed and integrated protections are implemented throughout the lifecycle of each process, program, and information system. For example, the implementation of

¹⁷DHS-OIG, *Management Oversight and Component Participation Are Necessary to Complete DHS' Human Resource Systems Consolidation Effort*, (OIG-10-99, July 2010)

¹⁸ DHS-OIG, *DHS' Progress in Disaster Recovery Planning for Information Systems* (OIG-09-60, April 2009).

¹⁹ DHS-OIG, *Management of DHS' Data Center Consolidation Initiative Needs Improvement*, (OIG-10-120, September 2010).

Homeland Security Presidential Directive -12, Policy for a Common Identification Standard for Federal Employees and Contractors, was especially challenging. The department was required to grant the necessary security rights and privileges to users so they could access the department’s facilities and networks, but still had to protect the confidentiality and privacy of its users and data.²⁰

In July 2010, we reported that ICE demonstrated an organizational commitment to privacy compliance by appointing a privacy officer and establishing the ICE Privacy Office.²¹ However, we identified areas for improvement. Specifically, to strengthen its privacy stewardship ICE needed to develop and implement job-related privacy training and oversight to safeguard PII in program operations and establish penalties for violations that correspond with DHS privacy rules of conduct.

IT Management Scorecard

The following scorecard demonstrates where DHS’ IT management functions have been strengthened. This high-level assessment identifies progress in six IT management capability areas: IT budget oversight, IT strategic planning, enterprise architecture, portfolio management, capital planning and investment control, and IT security. These six elements were selected based on IT management capabilities required by federal and DHS guidelines for enabling CIOs to manage IT department-wide.

Based on the consolidated result of the six IT management capability areas, DHS has made “**moderate**” progress in IT Management overall.

| IT MANAGEMENT SCORECARD | |
|--|-------------------------------|
| <p>IT Budget Oversight: ensures visibility into IT spending and alignment with the strategic IT direction.</p> | <p>Modest Progress</p> |
| <p>The DHS CIO has made improvements in managing department-wide IT budgets in accordance with the <i>Clinger-Cohen Act</i>²² and the department’s mission and policy guidance. The DHS 2009-2013 IT Strategic Plan emphasizes the importance of Component IT spending approval by either the Component-level CIO or the DHS CIO. However, gaining a department-wide view of IT spending was difficult due to some Component CIOs not having sufficient budget control and insight. For example, our 2010 report²³ on the U.S. Immigration and Customs Enforcement found that although the Office of the</p> | |

²⁰ DHS-OIG, *Resource and Security Issues Hinder DHS’ Implementation of Homeland Security Presidential Directive 12* (OIG-10-40, January 2010).

²¹ DHS-OIG, *Immigration and Customs Enforcement Privacy Stewardship* (OIG-10-100, July 2010).

²² *Clinger-Cohen Act of 1996*, Public Law 104-106, Division E, February 10, 1996.

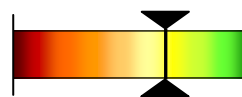
²³ DHS-OIG, *Immigration and Customs Enforcement Information Technology Management Progresses But Challenges Remain*, (OIG-10-90, May 2010).

IT MANAGEMENT SCORECARD

Chief Information Officer has oversight of information technology spending, its budget planning process did not capture all component information technology needs. As a result, the OCIO has limited ability to proactively manage and administer all IT resources and assets. Due to the limited benefits realized, IT Budget Oversight has made “modest” progress.

IT Strategic Planning: helps align the IT organization to support mission and business priorities.

Moderate Progress



An effective IT strategic plan establishes an approach to align resources and provides a basis for articulating how the IT organization will develop and deliver capabilities to support mission and business priorities. In January 2009, the department finalized its IT Strategic Plan, which aligns IT goals with overall DHS strategic goals. The plan also identifies technology strengths, weaknesses, opportunities, and threats. Due to the finalization and communication of the DHS IT Strategic Plan and plans to align IT with the department’s goals, this area has made “moderate” progress.

Enterprise Architecture: functions as a blueprint to guide IT investments for the organization.

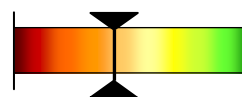
Moderate Progress



The *Clinger-Cohen Act* requires that CIOs develop and implement an integrated IT architecture for the agency to avoid the risk that systems will be duplicative, not well integrated, and limited in optimizing mission performance. The DHS IT Strategic Plan identifies a performance measure for the percentage of IT investments reviewed and approved through the Enterprise Architecture Board. This should further promote and enforce alignment of IT investments across the department. The department has shown “moderate” progress in implementing its enterprise architecture.

Portfolio Management: improves leadership’s ability to understand interrelationships between IT investments and department priorities and goals.

Modest Progress



The DHS OCIO has made “Modest” progress in establishing the department’s portfolio management capabilities as instructed by OMB Circular A-130.²⁴ The DHS portfolio management program aims to group related IT investments into defined capability areas to support strategic goals and missions. Portfolio management improves leadership’s visibility into relationships among IT assets and department mission and goals across

²⁴ Office of Management and Budget Circular A-130, Transmittal 4, *Management of Federal Information Resources*, November 2000.

IT MANAGEMENT SCORECARD

organizational boundaries.

The DHS IT Strategic Plan identifies a goal to effectively manage IT capabilities and implement cross-departmental IT portfolios that enhance mission and business performance. Although progress is being made, the department has not identified fully opportunities to standardize, consolidate, and optimize the IT infrastructure. Based on the limited benefits realized, the department has shown “modest” progress in implementing department-wide portfolio management.

Capital Planning and Investment Control: improves the allocation of resources to benefit the strategic needs of the department.

Moderate Progress



The *Clinger-Cohen Act* requires that departments and agencies create a capital planning and investment control (CPIC) process to manage the risk and maximize the value of IT acquisitions. The CPIC process is intended to improve the allocation of resources to benefit the strategic needs of the department. As part of the CPIC process, agencies are required to submit business plans for IT investments to OMB demonstrating adequate planning.

To address this requirement, DHS’ IT Strategic Plan communicated the importance of following the IT investment guidance provided by DHS management directive 0007.1.²⁵ This directive supports and expands on the Act’s requirement for technology, budget, financial, and program management decisions. The department has made “moderate” progress with respect to allocation of resources to benefit its strategic needs.

IT Security: ensures protection that is commensurate with the harm that would result from unauthorized access to information.

Moderate Progress



DHS IT security is rated at “moderate,” for progress made during the last 4 years in compliance with FISMA. OMB Circular A-130 requires agencies to provide protection that is commensurate with the risk and magnitude of the harm that would result from unauthorized access to information and systems assets or their loss, misuse, or modification. Regarding intelligence systems, information security procedures have been documented and controls have been implemented, providing an effective level of systems security.

²⁵ DHS Management Directive 0007.1: *Information Technology Integration and Management* March 2007.

EMERGENCY MANAGEMENT

FEMA’s mission is to support citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards. The Post-Katrina Emergency Management Reform Act of 2006 (Post-Katrina Reform Act),²⁶ enacted to address shortcomings exposed by Hurricane Katrina, expanded the scope of the agency’s mission, enhanced FEMA’s authority, and gave it primary responsibility for the four phases of comprehensive emergency management: preparedness, response, recovery, and mitigation.

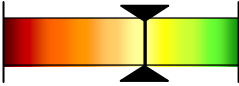
In March 2008, we released a report on FEMA’s progress in addressing nine key preparedness areas related to catastrophic disasters: overall planning, coordination and support, interoperable communications, logistics, evacuations, housing, disaster workforce, mission assignments, and acquisition management.²⁷ FEMA’s progress in these areas ranged from limited to moderate. In August 2010, we issued an update of our assessment and determined that FEMA has moved beyond limited progress in all areas, achieved modest progress in 2 areas, moderate progress in 7 areas, and substantial progress in 1 area (Mitigation was added as an additional key area).²⁸

In our FY2010 reports, we continued our focus on FEMA’s logistics systems, contracting practices, processes and procedures for individual and public assistance, and mitigation efforts.

Emergency Management

The following scorecard highlights FEMA’s progress in three key areas: logistics, housing, and mitigation.

Based on the consolidated result of the three areas presented here, as well as progress made in acquisition management and disaster grants management, FEMA has made “**moderate**” progress in the area of Emergency Management.

| EMERGENCY MANAGEMENT SCORECARD | |
|---|--|
| Logistics | Moderate Progress  |
| When disaster strikes, FEMA must be prepared to quickly provide goods and services to help state and local governments respond to the disaster. FEMA’s response in past | |

²⁶ Public Law 109-295, Title VI – National Emergency Management, of the *Department of Homeland Security Appropriations Act of 2007*.

²⁷ DHS-OIG, *FEMA’s Preparedness for the Next Catastrophic Disaster*, (OIG-08-34, March 2008).

²⁸ DHS-OIG, *FEMA’s Preparedness for the Next Catastrophic Disaster – An Update*, (OIG-10-123, September 2010).

EMERGENCY MANAGEMENT SCORECARD

disasters has demonstrated that when this function is lacking, disaster survivors face increased suffering. As a result of a congressionally mandated reorganization in 2007, FEMA created the Logistics Management Directorate, now within Response and Recovery. Beyond the structural reorganization, FEMA has been proactive in logistical improvements; however, more remains to be done.²⁹

FEMA has made great strides to improve its logistics capability by: (1) increasing staffing levels; (2) training and developing personnel; (3) enhancing coordination among federal, state, and local governments, nongovernmental organizations, and the private sector; (4) developing plans and exercises to improve readiness; (5) utilizing interagency agreements and contracts for needed commodities; (6) conducting meetings and teleconferences with logistics partners; and (7) reviewing and evaluating performance.

Despite FEMA's progress, corresponding improvements by many state and local governments have lagged behind due to staffing and budget restrictions. FEMA's logistics function is also hampered by the inability of its information systems to communicate directly with the systems of its federal partners. FEMA has several information systems it uses in its logistics function; which can lead to stovepipes and slow down response time. FEMA plans to have its systems interconnected by the end of the logistics transformation that is projected to be complete in 2014.

Housing

Moderate Progress



Since 2009, FEMA has made moderate progress in its disaster housing plans and operations. These improvements include progress in implementing the *National Disaster Housing Strategy*,³⁰ planning for the purchase, tracking and disposal of temporary housing units; and strengthening state and local commitment to house affected disaster survivors. FEMA has reorganized its Individual Assistance Division to address these action areas.

In January 2009, FEMA released the *National Disaster Housing Strategy*, which summarized FEMA's disaster housing process, including sheltering and housing capabilities, principles and policies. The Strategy has several components including the creation of a National Disaster Housing Task Force; the development of a Disaster Housing Implementation Plan; and a Comprehensive Concept of Operations. On March 16, 2010, the Office of Management and

²⁹ DHS-OIG, *FEMA's Logistics Management Process for Responding to Catastrophic Disaster*, (OIG-10-101, July 2010).

³⁰ FEMA's National Disaster Housing Strategy can be accessed at <http://www.fema.gov/pdf/emergency/disasterhousing/NDHS-core.pdf>.

EMERGENCY MANAGEMENT SCORECARD

Budget approved the Disaster Housing Implementation Plan. FEMA plans to release the Comprehensive Concept of Operations immediately following the release of the National Disaster Recovery Framework. FEMA developed a Non-Congregate Housing Program that uses hotels, motels or federally-owned unoccupied housing units as a sheltering resource. However, the program's success depends on leveraging the full capabilities of the federal government, state and local governments, the private sector, members of the community, and disaster survivors.

In March 2009, FEMA testified that it would consider the use of travel trailers only as a last resort when a state specifically requests them. In light of that decision, FEMA continues working to develop alternative forms of temporary housing. FEMA is working on separate projects with the Department of Housing and Urban Development (HUD) and seven alternative housing manufacturers to develop these housing units. This year, FEMA began an effort to sell more than 101,000 excess temporary housing units through whole-storage site sales conducted by the U.S. General Services Administration (GSA) online auctions. When the auctions closed in January 2010, FEMA had sold most of its excess inventory. The purchasers are in the process of removing the housing units, and FEMA anticipates that all storage sites will be closed by the end of FY 2011.

FEMA has developed two approaches to strengthen how state and local governments assist disaster survivors with temporary housing. The first approach is the development of state disaster housing taskforces, which are State entities that are assisted by FEMA to develop best practices, operational guidance and a standardized housing plan for unique disaster housing needs. The second approach is to work with state and local governments to identify temporary group housing sites. However, each approach has specific limitations, such as insufficient numbers of experienced disaster housing staff, limited federal and state funding, and poor coordination with state and local governments.

In addition to these areas, we are concerned that FEMA has not clearly defined its roles and responsibilities with regard to the long-term housing needs of disaster survivors (i.e., beyond the standard 18 months of assistance).

Mitigation

Moderate Progress



Hazard mitigation is a strategic component of our nation's integrated approach to emergency management. Mitigation provides a critical foundation to reduce loss of life and property by closing vulnerabilities and avoiding or lessening the impact of a disaster, leading to safer, more resilient communities. As noted in the 2010 Quadrennial Homeland Security Review Report,

EMERGENCY MANAGEMENT SCORECARD

“...the strategic aims and objectives for ensuring resilience to disasters are grounded in the four traditional elements of emergency management: hazard mitigation, enhanced preparedness, effective emergency response, and rapid recovery. Together, these elements will help create a Nation that understands the hazards and risks we face, is prepared for disasters, and can withstand and rapidly and effectively recover from the disruptions they cause.”

Although FEMA continues to improve its capacity and capability to lead an integrated national approach to hazard mitigation, there are a number of strategic and operational challenges that must be addressed in the years ahead. These challenges will require a focused and systematic effort by key mitigation partners and stakeholders at the federal, state, and local levels.

Challenge: Develop integrated national hazard mitigation strategy

The FY 2010 Quadrennial Homeland Security Review defines broad national objectives for mitigation:

- Reduce the vulnerability of individuals and families: Improve individual and family capacity to reduce vulnerabilities and withstand disasters.
- Mitigate risks to communities: Improve community capacity to withstand disasters by mitigating known and anticipated hazards.

The challenge for FEMA is to translate these objectives into an integrated national hazard mitigation strategy. There is no national consensus on how to address hazard mitigation as part of FEMA’s overall preparedness for catastrophic disasters. This is reflected in the fact that hazard mitigation was not included as a component of the initial Target Capabilities List (TCL), although FEMA states that the targeted capabilities define all-hazards preparedness and provide the basis to assess preparedness and improve decisions related to preparedness investments and strategies.³¹

Challenge: Improve local hazard mitigation planning process

The Disaster Mitigation Act of 2000 (P.L. 106-390) amended the Stafford Act to establish specific requirements for state and local hazard mitigation plans. Today, most states, major counties, and cities have active mitigation plans in place.

The challenge going forward, however, is to improve the quality and impact of this mitigation planning enterprise, and, ultimately, to reduce disaster losses and expenditures

³¹ Target Capabilities List, page 5, <http://www.fema.gov/pdf/government/training/tcl.pdf>.

EMERGENCY MANAGEMENT SCORECARD

beyond what they would have otherwise been.

State and local hazard mitigation officials continue to report large gaps in the capacity and will of communities to plan and implement mitigation strategies. This is important because while FEMA provides grant funds and administrative support to the state, it is the local hazard mitigation professionals and stakeholders who develop and implement mitigation projects. When communities lack capacity to mitigate hazards, FEMA's ability to ensure an effective national approach to hazard mitigation is diminished.

To improve local hazard mitigation planning, FEMA should enhance community outreach and awareness, engage stakeholders in preparing and reviewing state and local hazard mitigation plans, simplify and standardize benefit cost processes, and enhance state and local risk assessment and analysis capabilities.

Challenge: Improve hazard mitigation outcomes

FEMA faces multiple challenges in its efforts to improve hazard mitigation outcomes. The most important challenge lies in the scope and complexity of the mitigation landscape—thousands of entities and individuals must work together in a loosely coordinated effort to achieve nationally significant results. Mitigation stakeholders include floodplain managers, risk managers, insurers, property developers, homeowners, government officials, environmentalists, and the public at large bring conflicting priorities and interests to any discussion of mitigation. Further, FEMA is limited by statute to the promotion of effective mitigation practices and lacks the authority to compel property owners to mitigate floods or other hazards. This is true even when hazard mitigation appears desperately needed, as in the case of repetitively flooded properties.

To improve hazard mitigation outcomes, FEMA should look for opportunities to reduce the complexity and scope of mitigation planning guidance to the extent possible to remain consistent with legislative intent while meeting the requirements of state and local mitigation. FEMA should ensure monitoring and follow-up of mitigation actions in state and local plans, integrate hazard mitigation into Emergency Support Function activities and preliminary damage assessments, and assess ongoing mitigation programs for gaps and opportunities for improvement.

GRANTS MANAGEMENT

FEMA assists communities in responding to and recovering from disasters. FEMA provides disaster assistance to communities through the Public Assistance Grant Program, the Hazard Mitigation Grant Program, and the Fire Management Assistance Grant Program. Under each of these grant programs, the affected State is the grantee, and the State disburses funds to

eligible subgrantees. FEMA also awards grants to state and local governments; territories; tribal governments; and private, public, profit, and nonprofit organizations to enhance preparedness, protection, response, recovery, and mitigation capabilities throughout the Nation. However, improvements are needed in FEMA's grants management and oversight infrastructure to ensure effective monitoring of grantees.

The Post Katrina Emergency Management Reform Act (PKEMRA) of 2006 centralized most of DHS' grant programs under FEMA's Grant Programs Directorate (GPD). GPD administers 52 distinct disaster and non-disaster grant programs and each year awards between 6,000 and 7,000 individual grants, totaling \$7 billion to \$10 billion each year. GPD is currently reviewing its basic functions with respect to four key principles: (1) to administer FEMA's grant programs responsibly and economically, (2) to build and sustain the internal capabilities to ensure success, (3) to show how each grant dollar improves the nation's capabilities and provides a strong return on investment, and (4) to carry out its mission within a new and evolving FEMA structure. Given the billions of dollars appropriated annually for preparedness, disaster, and non-disaster grant programs, GPD needs to ensure that internal controls are in place and adhered to, and that grant recipients are sufficiently monitored to achieve successful outcomes. GPD should continue refining its risk-based approach to awarding and monitoring preparedness grants to ensure that the most vulnerable areas and assets are as secure as possible. Sound risk management principles and methodologies will help GPD prepare for, respond to, recover from, and mitigate acts of terrorism and natural disasters.

Grants Management

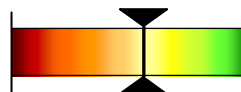
The following scorecard highlights the department's progress in two key areas: disaster and non-disaster grants management. FEMA is taking steps to improve its grant policies, procedures, systems, and processes which when developed and implemented should strengthen its grants management and oversight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

Based on the consolidated result of the two areas presented here, FEMA has made "**modest**" progress in the area of Grants Management.

GRANTS MANAGEMENT SCORECARD

Disaster Grants Management

Moderate Progress



In FY 2009, we issued 51 financial assistance (subgrant) audit reports, identifying more than \$138 million in questioned costs and over \$15 million in funds that could be put to better use. As of August 9, 2010, we had issued 39 subgrant audit reports in FY 2010, with nearly \$80 million in questioned costs and nearly \$37 million in funding that could be deobligated or collected and be put to better use.

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 plan to issue a report in FY 2011 that recaps the reports we issued in FY 2010 and presents some of the most common problems that lead to questioned costs, including inconsistent interpretation of policies by FEMA personnel, grantee and subgrantee non-compliance with the federal regulations governing disaster grants and federal policy on grants management in general, and the lack of grantee monitoring of subgrantee activities.

Non - Disaster Grants Management

Modest Progress



FEMA faces challenges in mitigating redundancy and duplication among preparedness grant programs. The preparedness grant application process risks being ineffective because FEMA does not compare and coordinate grant applications across preparedness programs. Barriers at the legislative, departmental, and state levels impede FEMA's ability to coordinate these 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 efficacy of these grant programs which FEMA agreed with and outlined plans and actions to implement the recommendations.

Public Law 110-53, *Implementing Recommendations of the 9/11 Commission Act of 2007* required the Office of Inspector General 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 three complete years since the law was enacted, the states we audited generally did an efficient and effective job of administering the grant management program requirements, distributing grant funds, and ensuring that all the available funds were used.

However, during FY 2010, we issued audit reports in which states, as grantees, were not

GRANTS MANAGEMENT SCORECARD

sufficiently monitoring subgrantee compliance with grant terms and could not clearly document critical improvements in preparedness as a result of grant awards. Issued audit reports on homeland security grants management included Maryland, Missouri, South Carolina, and West Virginia. These entities generally did an efficient and effective job of administering the grant funds; however, in addition to problems with performance measurement and subgrantee monitoring, other areas that needed improvement included financial documentation and reporting, compliance with procurement and inventory requirements, and identification of long-term capability sustainment options. We also issued seven draft reports in FY 2010 that will be finalized in early FY 2011.

FINANCIAL MANAGEMENT

DHS continued to improve financial management in FY 2010, but challenges remain. In FY 2010 our Independent auditor performed an integrated financial statement and internal control over financial reporting audit that was limited to the DHS consolidated balance sheet and statement of custodial activity. As in previous years, our Independent auditor was unable to provide an opinion on those statements because the department could not provide sufficient evidence to support its financial statements or represent that financial statement balances were correct. Additionally, the Independent auditor were unable to perform procedures necessary to express an opinion on DHS' internal controls over financial reporting of the balance sheet and statement of custodial activity due to the pervasiveness of the department's material weaknesses.

Although the department continued to remediate material weaknesses and reduced the number of conditions contributing to the disclaimer of opinion on the financial statements, all six material weakness conditions from FY 2009 were repeated in FY 2010. Furthermore, the Independent auditor identified four department-wide control environment weaknesses that have a pervasive impact on the effectiveness of internal controls over consolidated financial reporting, challenges two through four are repeated from FY 2009. Specifically:

- Development and implementation of effective information and communication processes to help ensure that technical accounting issues are identified, analyzed, and resolved in a timely manner. For example, development of an accounting position and/or responses to our questions at Customs and Border Protection (CBP), FEMA, and Transportation Security Administration (TSA) at various times throughout the audit is often a time-consuming process that spans several months, even for less complex matters;
- Generally, the components continue to be dependent on the external financial statement audit to discover and resolve technical accounting issues;

- Field and operational personnel do not always share responsibilities for, or are not held accountable for, financial management matters that affect the financial statements, including adhering to accounting policies and procedures and performing key internal control functions in support of financial reporting; and
- The department's financial Information Technology system infrastructure is aging and has limited functionality, which is hindering the department's ability to implement efficient corrective actions and produce reliable financial statements that can be audited. Weaknesses in the general control environment are interfering with more extensive use of IT application controls to improve efficiencies in operations and reliability of financial information.

The Independent auditor noted that the DHS civilian components continued to make some progress in the remediation of IT findings that were reported in FY 2009. The Independent auditor noted that the department closed approximately 30 percent of prior year IT findings. In FY 2010 the Independent auditor issued approximately 140 findings, of which more than 60 percent are repeated from last year. Further, nearly one-third of our repeat findings were for IT deficiencies that management represented were corrected during FY 2010. Disagreement with management's self-assessment occurred almost entirely at FEMA.

In FY 2010, TSA corrected the IT controls and systems functionality weakness condition, while weakness conditions remained unchanged at FEMA, ICE, CBP, USCIS, and Federal Law Enforcement Training Center (FLETC). The weakness conditions at FEMA and ICE are more severe than the conditions at CBP, USCIS, and FLETC.

The remaining significant component-level challenges preventing the department from obtaining an opinion on its consolidated balance sheet and statement of custodial activity are primarily at the Coast Guard. In FY 2010, 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 completeness, existence, and accuracy of Property, Plant, & Equipment (PP&E), actuarial liabilities, and fund balance with Treasury. In addition to its planned FSTAR initiatives for FY 2010, the Coast Guard performed remediation efforts over discrete elements of its balance sheet. This "balance sheet strategy" was designed to achieve additional account balance assertions. As a result, the Coast Guard was able to assert to more than \$43 billion of its balance sheet. FSTAR calls for continued remediation of control deficiencies and reconciliation of balances in FY 2011.

Anti-Deficiency Act Violation:

As of September 30, 2010, the department reported 9 instances of potential *Anti-Deficiency Act* (ADA) violations that are in various stages of review. Based on reviews completed in FY 2009 and FY 2010, the department has requested that the OIG perform numerous ADA audits. Currently, the OIG is conducting audits on the following cases of potential ADA violations:

1. National Protection and Programs Directorate's (NPPD) Shared Services process in FY 2006.
2. Coast Guard's FY 03 – FY 07 Shore Facility Operating Expenses.
3. United States Secret Service (USSS) salaries and expenses for presidential candidate nominee protection.
4. Coast Guard's FY 04, FY 05, and FY 07 Acquisition, Construction, and Improvement Appropriation.

The OIG concurred with management's assessment³² that FLETC's reclassification of the second dormitory as a capital lease caused the required obligation for this lease to exceed FLETC's appropriation authority, resulting in an ADA violation.

We noted that the DHS OCFO has established policy and standards for the administrative control of funds (*DHS Financial Management Policy Manual*, Section 2.5, Updated February 2010).

Financial Management Scorecard

The following scorecard presents the status of DHS' effort to address internal control weaknesses in financial reporting that were identified in FY 2009. The scorecard is divided into two categories: (1) Military – Coast Guard, and (2) Civilian – all other DHS components. The scorecard lists the six material weaknesses identified during the independent audit of the FY 2009 DHS consolidated balance sheet and statement of custodial activity. These weaknesses continued to exist throughout FY 2010 and were again noted in the FY 2010 Independent Auditors' report; however Civilian Components reduced the severity of several material weakness conditions. For a complete description of the internal control weaknesses identified in the FY 2009 audit, see OIG-10-11.³³ To determine the status, we compared the material weaknesses reported by the Independent auditor in FY 2009 with those identified in FY 2010.³⁴ The scorecard does not include other financial reporting control deficiencies identified in FY 2010 that do not rise to the level of a material weakness, as defined by the American Institute of Certified Public Accountants.

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


³² DHS-OIG, *FLETC Leases for Dormitories 1 and 3*, (OIG-10-02, October 2009).

³³ DHS-OIG, *Independent Auditor's Report on DHS' FY 2009 Financial Statements and Internal Control over Financial Reporting*, (OIG-10-11, November 2009).



³⁴ DHS-OIG, *Independent Auditor's Report on DHS' FY 2010 Financial Statements and Internal Control Over Financial Reporting*, (OIG-11-09, November 2010).

FINANCIAL MANAGEMENT SCORECARD


Financial Management and 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. Financial management is the planning, directing, monitoring, organizing, and controlling of financial resources, including program analysis and evaluation, budget formulation, execution, accounting, reporting, internal controls, financial systems, grant oversight, bank cards, travel policy, appropriation-related Congressional issues and reporting, working capital funds, and other related functions.

| | | |
|-----------------|--|---|
| Military | Limited Progress |  |
| | <p>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 <i>Financial Strategy for Transformation and Audit Readiness</i>, 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 2009 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.</p> <p>The Coast Guard has demonstrated limited progress in remediating the numerous internal control weaknesses identified by the Independent auditor during FY 2009. In FY 2010, the Coast Guard completed its planned corrective actions over certain internal control deficiencies, which allowed management to make assertions on the completeness and accuracy of certain account balances. However, many of the corrective actions outlined in the FSTAR are scheduled to occur after FY 2010, and consequently many of the financial reporting weaknesses reported in prior years remained as of the fiscal year end.</p> <p>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 <i>Federal Financial management Improvement Act</i>. Additionally, the organization lacks effective policies, procedures, and internal controls to ensure that data supporting financial statements is complete and accurate, and technical accounting issues are identified, analyzed, and resolved in a timely manner.</p> | |

FINANCIAL MANAGEMENT SCORECARD

| | | |
|---|--------------------------|---|
| Civilian | Moderate Progress |  |
| <p>In FY 2009, the Independent auditor identified department-wide control weaknesses that have a pervasive effect on the effectiveness of internal controls over consolidated financial reporting. The Independent auditor also found financial reporting internal control deficiencies for FEMA, TSA, and CBP. The deficiencies at FEMA and TSA were more significant than deficiencies at CBP. Taken together, these deficiencies contributed to a departmental material weakness.</p> <p>During FY 2010, the department made moderate progress overall in addressing the department-wide control weaknesses over consolidated financial reporting. The Independent auditor noted that during FY 2010, TSA demonstrated some progress by hiring accounting personnel and completing reconciliation of its balance sheet accounts. Additionally, TSA addressed matters that have led to misstatements in the financial statements in previous years. In addition, CBP and FEMA took positive steps in FY 2010 to correct control deficiencies that were reported in prior years. Because of the remediation efforts at CBP, TSA and FEMA, the Independent auditor downgraded the severity of the control deficiencies. As a result, TSA no longer contributes to the qualifications on the Independent Auditors' report. These combined internal control deficiencies contributed to the department's financial management and reporting material weakness in FY 2010.</p> | | |
| <p>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.</p> | | |
| Military | Limited Progress |  |
| <p>During 2009, the Independent auditor identified 20 IT general control deficiencies, 11 of which were repeat findings from the prior year. The most significant IT deficiencies 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. These deficiencies at the Coast Guard contributed to the FY 2009 departmental material weakness over IT controls and financial systems functionality.</p> <p>The Coast Guard has demonstrated limited progress in FY 2010 by remediating eight general control weaknesses identified in previous</p> | | |

FINANCIAL MANAGEMENT SCORECARD

| | | |
|-----------------|--|---|
| | <p>years. Specifically, the Coast Guard demonstrated improvement in its user recertification process, data center physical security, and scanning for system vulnerabilities. These remediation efforts enabled the Independent auditor to expand testwork into areas that were previously not practical to audit due to the pervasiveness of IT general control weaknesses.</p> <p>As a result of the expanded IT testing in FY 2010, the auditors have identified new weaknesses. Of the 28 IT control deficiencies the auditors identified during FY 2010, 10 are repeat findings from the prior year and 18 are new findings.</p> <p>One key area that remains a challenge for the Coast Guard is its core financial system configuration management process. For 2010, the auditors again noted that the configuration management process is not operating effectively, and continues to present risks to DHS financial data confidentiality, integrity, and availability. The auditors reported that financial data in the general ledger may be compromised by automated and manual changes that are not properly 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 from the beginning. The auditors noted that while the Coast Guard implemented a new script change management tool during the second half of FY 2010, other deficiencies in the IT script control environment existed throughout the fiscal year.</p> | |
| Civilian | Limited Progress |  |
| | <p>During FY 2009, the Independent auditor identified three areas that continued to present risks to the confidentiality, integrity, and availability of DHS' financial data: 1) excessive access to key DHS financial applications, 2) application change control processes that are inappropriate, not fully defined or followed, and are ineffective, and 3) security management practices that do not fully and effectively ensure that financial systems are certified, accredited, and authorized for operation prior to implementation. During FY 2009, FEMA and ICE contributed to an overall material weakness in IT general and applications control, while CBP, FLETC, TSA, and USCIS all had significant deficiencies in this area.</p> <p>For FY 2010, DHS has made limited progress overall in correcting the IT general and applications control weaknesses identified in the FY 2009</p> | |

FINANCIAL MANAGEMENT SCORECARD

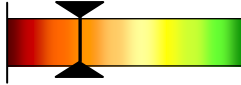
Independent Auditor’s report. The Independent auditor identified that TSA eliminated its significant deficiency. However, FEMA, ICE, CBP, FLETC, and USCIS continued to contribute to the departmental IT controls and system functionality material weakness condition. Control deficiencies at FEMA and ICE were more severe than deficiencies at CBP, FLETC, and USCIS.

Additionally, FEMA may not have a complete understanding of its control deficiencies because FEMA reported that it closed 28 information controls and system functionality weakness conditions but the Independent auditor concurred with management’s conclusion on only 5 of the conditions reported as closed.

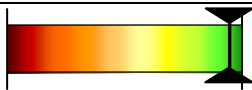

The auditors noted that many of the financial systems in use at DHS components have been inherited from the legacy agencies and have not been substantially updated since DHS’ inception. As a result, ongoing financial system functionality limitations are contributing to the department’s challenges in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

The FY 2010 Independent Auditor’s report identified the following weaknesses in the IT control areas that increase the 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 auditor noted that in some cases financial system functionality is inhibiting DHS’ ability to implement and maintain or install internal controls, and that financial system functionality limitations contribute to the department’s other material weaknesses.

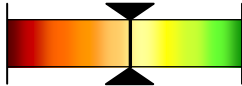
Fund Balance with Treasury (FBWT): FBWT represents accounts held at the Treasury from which an agency can make disbursements to pay for its operations. Regular reconciliation of an agency’s FBWT records with Treasury is essential to monitoring and safeguarding these funds, improving the integrity of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

| | | |
|-----------------|---|---|
| Military | Modest Progress |  |
| | <p>In FY 2009, the Independent auditor identified several internal control weaknesses related to FBWT which contributed a material weakness in this area at the Coast Guard. Among the internal weakness conditions</p> | |

FINANCIAL MANAGEMENT SCORECARD

| | | |
|---|--|---|
| | <p>the auditors noted in FY 2009 was that the Coast Guard had not developed a comprehensive process, to include effective internal controls, to ensure that FBWT transactions are recorded in the general ledger timely, completely, and accurately.</p> <p>As of the end of FY 2010, the Coast Guard's FBWT represented approximately 11 percent of the department's total FBWT. Overall, the Coast Guard has demonstrated modest progress in addressing the material weaknesses noted during FY 2010. Although the Coast Guard corrected some FBWT control deficiencies, additional corrective actions are planned for FY 2011. Consequently, most of the FY 2009 weakness conditions were reported again in FY 2010.</p> <p>One of the key factors contributing to the FBWT material weakness is that the Coast Guard has not designed and implemented accounting processes, including a financial system that complies with federal financial systems requirements, as defined in the OMB Circular No. A-127, <i>Financial Management Systems</i>, to support the FY 2010 FBWT activity and balance.</p> | |
| Civilian | N/A |  |
| | <p>No control deficiencies related to FBWT were identified at the civilian components in FY 2010. Corrective actions implemented in previous years continued to be effective throughout FY 2009 and FY 2010.</p> | |
| <p>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.</p> | | |
| Military | Limited Progress |  |
| | <p>The Coast Guard maintains approximately 51 percent of the department's PP&E, including a large fleet of boats and vessels. The Coast Guard also maintains significant quantities of operating materials and supplies (OM&S), which consist of tangible personal property to be consumed in normal operation of service marine equipment, aircraft, and other equipment.</p> <p>In FY 2009, internal control weaknesses related to PP&E and OM&S at the Coast Guard contributed to the departmental material weaknesses.</p> | |

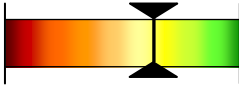
FINANCIAL MANAGEMENT SCORECARD

| | | |
|-----------------|---|---|
| | <p>For FY 2010, the Coast Guard has demonstrated limited progress overall in correcting internal control weaknesses related to PP&E identified in the Independent Auditor’s report in FY 2009. In addition to its planned FSTAR initiatives for FY 2010, the Coast Guard performed additional remediation efforts over discrete elements of its balance sheet. This "balance sheet strategy" was designed to achieve additional account balance assertions. As a result, the Coast Guard implemented additional measures to resolve the OM&S portion of the material weakness ahead of the planned FSTAR remediation milestone. However, the Coast Guard was unable to accomplish all aspects of its planned remediation efforts. Moreover, most of the corrective actions included in the FSTAR are scheduled to occur over a number of years. Consequently, many of the material weakness conditions noted during FY 2010 also existed in FY 2009. For example, one of the conditions the auditors identified, which is a repeat deficiency from prior years, is that the Coast Guard has not established its beginning PP&E balance necessary to prepare the fiscal year-end balance sheet. The Coast Guard conducted inventory procedures during FY 2010 to assist management in substantiating the existence and completeness of PP&E balances; however, those procedures were not performed over all asset classes (e.g real property).</p> <p>The Independent auditor also noted that the Coast Guard has had difficulty establishing its opening PP&E balances primarily because of poorly designed policies, procedures, and processes implemented more than a decade ago, 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, and now the Coast Guard is faced with the formidable challenge of performing a retroactive analysis in order to properly establish the existence, completeness, and accuracy of PP&E. Furthermore, the fixed asset module of the Coast Guard’s CAS is not updated timely for effective tracking and reporting of PP&E on an ongoing basis. As a result, the Coast Guard is unable to accurately account for its PP&E, and provide necessary information to DHS OFM for consolidated financial statement purposes.</p> | |
| Civilian | Moderate Progress |  |
| | <p>During FY 2009, CBP and TSA contributed to an overall material weakness in PP&E, while ICE, NPPD, TSA, and USCIS all had significant deficiencies in this area.</p> <p>During FY 2010, DHS demonstrated moderate progress overall in</p> | |

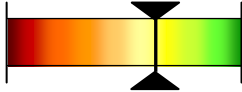

FINANCIAL MANAGEMENT SCORECARD

correcting internal control weaknesses related to PP&E identified in the Independent Auditor’s report in FY 2009. ICE, NPPD, and USCIS have fully corrected internal control weakness conditions related to PP&E, while CBP reduced the severity of its control deficiencies. Additionally, TSA completed the reconciliation of its PP&E accounts in FY 2010 and was able to assert that its PP&E balances at September 30, 2010 are fairly stated in the DHS FY 2010 *Annual Financial Report*. Although TSA made some progress in remediating control deficiencies, including having auditable beginning PP&E balance, it was unable to fully address all of the conditions that existed in FY 2009. Consequently, the overall severity of its internal control weakness conditions remained in FY 2010.

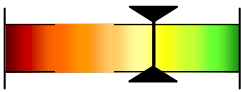
Actuarial and Other Liabilities: Liabilities represent the probable and measurable future outflow or other sacrifice of resources as a result of past transactions or events. The internal control weaknesses reported in this area are related to various types of liabilities, including accounts and grants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

| | | |
|---|--------------------------|--|
| Military | Moderate Progress |  |
| <p>The Coast Guard maintains medical, pension, and post-employment travel benefit programs that require actuarial computations to record related liabilities for financial reporting purposes. Other liabilities include accounts payable, environmental, and legal liabilities.</p> <p>In FY 2009, the Independent auditor noted a number of internal control deficiencies related to actuarial liabilities at the Coast Guard, which contributed to a material weakness for the department.</p> <p>During FY 2010, the Coast Guard demonstrated moderate progress overall by completing its planned corrective actions over selected internal control and reporting deficiencies that existed in this process in FY 2009. Specifically, remediation efforts associated with accounts payable, accrued payroll, pension, and medical liabilities allowed management to assert to the completeness and accuracy of over \$43 billion of accrued liabilities, which represents more than 50 percent of DHS’ total liabilities. However, management was unable to provide sufficient evidential matter that support transactions and balances related to environmental and other liabilities. Among the conditions that remained throughout FY 2010 is the Coast Guard has not implemented effective policies, procedures, and controls to ensure the completeness and accuracy of environmental liabilities.</p> | | |

FINANCIAL MANAGEMENT SCORECARD

| | | |
|---|-----------------------------|---|
| Civilian | Substantial Progress |  |
| <p>For FY 2009, the Independent auditor noted internal control weaknesses related to liabilities at FEMA and TSA.</p> <p>During FY 2010, the civilian components demonstrated substantial progress overall in remediating internal control weaknesses related to actuarial and other liabilities, with TSA fully remediating its control weakness condition. FEMA is recognized as the primary grant-making component of DHS and the FY 2010 Independent Auditor’s report noted that FEMA does not have sufficient policies and procedures in place to fully comply with the <i>Single Audit Act Amendments of 1996</i> and OMB Circular No. A-133, <i>Audits of States, Local Governments, and Non-profit Organizations</i>. As a result, FEMA continued in FY 2010 to contribute to the departmental actuarial and other liabilities material weakness condition.</p> | | |
| <p>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.</p> | | |
| Military | Limited Progress |  |
| <p>The Coast Guard has over 90 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.</p> <p>In FY 2009, the Independent auditor noted a number of internal control deficiencies related to budgetary accounts that contributed to a material weakness in this area for the department.</p> <p>For FY 2010, the Coast Guard has made limited progress in remediating the internal control weaknesses in this area. Many of the conditions that contributed to a material weakness in budgetary accounting at the Coast Guard in FY 2009 remained throughout FY 2010. For example, the FY 2009 Independent Auditors’ report noted that the policies, procedures, and internal controls over the Coast Guard’s process for validation and verification of some account balances are not effective to ensure recorded amounts are complete, valid, accurate, and proper approvals and supporting documentation are maintained. These weaknesses</p> | | |

FINANCIAL MANAGEMENT SCORECARD

| | | |
|-----------------|--|---|
| | continued to exist in FY 2010, and remediation of these conditions is not planned until after FY 2010. | |
| Civilian | Moderate Progress |  |
| | <p>For FY 2009, internal control weaknesses at CBP and FEMA contributed to a departmental budgetary accounting material weakness.</p> <p>During FY 2010, the department demonstrated moderate progress in correcting the budgetary accounting material weakness. FEMA improved its processes and internal controls over the obligation and monitoring process, but control deficiencies remain. Additionally, CBP implemented policies and procedures requiring the timely review and deobligation of funds when contracts have expired or are complete. However, CBP did not adhere to those policies and procedures. As a result, FEMA and CBP contributed to the departmental budgetary accounting material weakness condition.</p> | |

INFRASTRUCTURE PROTECTION

DHS has direct responsibility for leading, integrating, and coordinating efforts to protect 11 critical infrastructure and key resources (CI/KR) sectors: the chemical industry; commercial facilities; critical manufacturing; dams; emergency services; commercial nuclear reactors, materials, and waste; information technology; telecommunications; postal and shipping; transportation systems; and government facilities. In addition, DHS has an oversight role in coordinating the protection of seven sectors for which other federal agencies have primary responsibility. The seven sectors for which DHS has an oversight role are agriculture and food; the defense industrial base; energy; public health and healthcare; national monuments and icons; banking and finance; and water and water treatment systems. The requirement to rely on federal partners and the private sector to deter threats, mitigate vulnerabilities, or minimize incident consequences complicates protection efforts for all CI/KR. Combined with the uncertainty of the terrorist threat and other manmade or natural disasters, the implementation of protection efforts is a great challenge.

In our FY 2009 report, *Efforts to Identify Critical Infrastructure Assets and Systems*, we reported that the National Protection and Programs Directorate is in the process of acquiring the Infrastructure Information Collection System, a replacement for the National Asset Database.³⁵ It is envisioned that the Infrastructure Information Collection System will greatly reduce critical infrastructure risk management gaps by providing dynamic

³⁵DHS-OIG, *Efforts to Identify Critical Infrastructure Assets and Systems*, (OIG-09-86, June 2009).

information collection systems that include a range of relevant sources. In addition, the Infrastructure Information Collection System will allow relevant critical infrastructure partners from federal, state, local, and private entities to access various tools that house infrastructure data. We recently closed this recommendation because NPPD has made progress and the unclassified system is now in use. However, the classified system has not been implemented.

Concerning DHS efforts to protect the cyber infrastructure, we reported in June 2010 that the United States Computer Emergency Readiness Team (US-CERT) had made progress in implementing a cybersecurity program to assist federal agencies in protecting their information technology systems against threats.³⁶ However, US-CERT does not have appropriate enforcement authority to ensure that agencies comply with its mitigation guidance concerning threats and vulnerabilities. Additionally, US-CERT does not have sufficient staff to perform its 24x7 operations and to analyze security information timely. US-CERT had not developed a strategic plan and must improve its information sharing efforts with federal agencies. Finally, US-CERT does not have the capability to monitor federal cyberspace in real-time.

BORDER SECURITY

Securing the nation's borders from illegal entry of aliens and contraband, including terrorists and weapons of mass destruction, continues to be a major challenge. DHS apprehends hundreds of thousands of people and seizes large volumes of cargo entering the country illegally each year. The U.S. Customs and Border the DHS component responsible for securing the nation's borders at and between the ports of entry. To achieve this goal, CBP is implementing the Secure Border Initiative (SBI), a comprehensive multi-year approach intended to help secure the 7,000 miles of international borders that the United States shares with Canada and Mexico. The program, which began in November 2005, seeks to enhance border security and reduce illegal immigration through the use of surveillance technologies, increase staffing levels, increase domestic enforcement of immigration laws, and improve physical infrastructure along the nation's borders.

The technology component of SBI, referred to as SBInet, is a major acquisition program initiated to gain operational control of the borders by designing and deploying a new integrated system of technology, infrastructure, and personnel. The specific objective of SBInet is to provide Border Patrol command centers with the imagery and intelligence to detect, identify, and interdict illegal incursions at and between our land ports of entry. DHS' ability to monitor SBInet has been a continuing concern. Previously, we reported that DHS did not have the acquisition workforce required to adequately plan, oversee, and execute SBInet, and that CBP had not established adequate controls and effective oversight of

³⁶ DHS OIG, *U.S. Computer Emergency Readiness Team Makes Progress in Securing Cyberspace, but Challenges Remain* (OIG-10-94, June 2010).

contract workers responsible for providing SBI program support services.³⁷ Also, the Government Accountability Office identified significant risk of the SBInet program not meeting mission needs and the increased risk of unnecessary program costs resulting from time consuming system rework.³⁸ Because of these and other concerns related to the efficacy of the implementation of SBInet technologies, the Secretary, in January 2010, requested a department-wide reassessment of the program that will identify alternatives to the current SBInet strategy that may more efficiently and effectively meet border security needs. The Secretary subsequently froze all SBInet funding beyond the initial deployment to the Tucson and Ajo regions until the reassessment is complete.

In June 2010, we reported that CBP needed to improve its control of contractor activities on the SBI technology program. Specifically, program officials did not ensure that contractors maintained up-to-date information in the primary management tool designed to provide managers with advance information regarding potential cost overruns and program progress. In addition, program officials did not ensure that a program event was properly completed before progressing to the next event, and did not adequately document their review and acceptance of accomplishments and criteria at program events. CBP has a low number of government personnel assigned to oversee contractor activities, which increases the program office's risk that program cost and schedule are not adequately managed and that goals are not met. CBP has taken steps to improve SBI technology program oversight by using the defense Contracting Management Agency personnel to assist with contract administration and reissuing important program documentation.³⁹

CBP faces challenges in meeting small business subcontracting goals for the remainder of the Secure Border Initiative Net indefinite delivery, indefinite quantity contract. A change in CBP's acquisition strategy from acquiring technology to acquiring steel for border fence construction reduced opportunities for small business to participate in awards under the Secure Border Initiative Net contract. In response the prime contractor, Boeing, has implemented initiatives to improve small business participation in Secure Border Initiative Net subcontracts to achieve its subcontracting goals. Despite these initiatives, the contractor has not achieved the established goals for small business participation since the reporting period ended September 2007.⁴⁰

Additionally, we previously reported that DHS needs to focus on improving the policies, processes, and procedures that govern the management and care of its detainee population. Prior reviews of ICE's detention and removal operations identified deficiencies in the oversight of immigration detention facilities. ICE has made efforts to strengthen the oversight of ICE detention assets by establishing a Detention Facilities Inspection Group (DFIG). The DFIG provides ICE with an independent inspection arm dedicated to oversight

³⁷ DHS OIG, *Better Oversight Needed of Support Services Contractors in Secure Border Initiative Programs*, OIG-09-80, June 2009.

³⁸ Government Accountability Office, *Secure Border Initiative: DHS Needs to Reconsider Its Proposed Investment in Key Technology Program*, GAO-10-340, May 2010

³⁹ DHS OIG, *Controls Over SBInet Program Cost and Schedule Could Be Improved*, (OIG-10-96, June 2010).

⁴⁰ DHS OIG, *CBP Faces Challenges in Achieving Its Goals for Small Business Participation in Secure Border Initiative Network*, (OIG-10-54, February 2010).

of ICE's Detention and Removal Operations (DRO) program. ICE has contracted with private companies to provide on-site compliance verification of the Performance-Based National Detention Standards at all ICE detention facilities. Last year we reported that ICE could further improve documenting the transfer of immigrant detainees and ensuring they received timely medical screenings and physical examinations, required by detention standards.⁴¹ Additionally, ICE needed to determine whether its approach to detention facility bed space management was cost-effective.⁴² ICE has been responsive to the issues identified in the two reports and is implementing the recommendations to address these issues.

TRANSPORTATION SECURITY

The nation's transportation system is vast and complex. It consists of about 3.9 million miles of roads, over 100,000 miles of rail, almost 600,000 bridges, over 300 sea ports, over 2 million miles of pipeline, about 500 train stations, and over 5,000 public-use airports. The size of the transportation system, which moves millions of passengers and tons of freight every day, makes it both an attractive target for terrorists and difficult to secure. The nation's economy depends upon implementation of effective, yet efficient transportation security measures. The Transportation Security Administration is responsible for protecting the transportation system and ensuring the freedom of movement for people and commerce. Given the "open" environment, TSA must establish effective security strategies, while maintaining quick and easy access for passengers and cargo. Since its inception, TSA continues to face challenges with strengthening security for aviation, mass transit and other modes of transportation. Although TSA is making progress in addressing these challenges, more needs to be done.

Checkpoint and Checked Baggage

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*⁴³ requires TSA to prescribe requirements for screening or inspecting all passengers, goods, and property before entry into the sterile areas of an airport. Our undercover audit of checked baggage screener performance revealed that improvements are needed in the screening process to ensure that dangerous prohibited items that enter the checked baggage system are not cleared for loading onto a passenger aircraft.⁴⁴ We recently issued a classified report on our unannounced, covert testing which identified needed improvements for TSA's newly deployed and enhanced screening checkpoint technologies.⁴⁵ We evaluated Advanced Imaging

⁴¹ DHS-OIG, *Immigration and Customs Enforcement's Tracking and Transfers of Detainees*, (OIG-09-41, March 2009).

⁴² DHS-OIG, *Immigration and Customs Enforcement Detention Bedspace Management*, (OIG-09-52, April 2009).

⁴³ Public Law 107-71, November 19, 2001.

⁴⁴ DHS-OIG, *Audit of the Effectiveness of the Checked Baggage Screening System and Procedures Used to Identify and Resolve Threats*, (OIG-09-42, March 2009).

⁴⁵ DHS-OIG, *Evaluation of Newly Deployed and Enhanced Technology and Practices at the Passenger Screening Checkpoint* (OIG-10-75, March 2010).

Technology, Advanced Technology X-ray equipment, and Liquid Container Screening used to screen passengers or their carry-on items and tested Transportation Security Officer performance in checking passengers' travel documents.

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.

TSA could improve its efforts to secure air cargo during ground handling and transportation. We reviewed the effectiveness of the TSA’s efforts to secure air cargo while it is handled or transported on the ground, prior to being shipped on passenger aircraft.⁴⁶ We determined that personnel were sometimes accessing, handling, or transporting air cargo without the required background checks or training. The agency’s inspection process has not been effective in ensuring that requirements for securing air cargo during ground transportation are understood or followed. The inspection process has focused on quantity rather than outcomes and ensuring corrective actions. We reported that automated tools to assist inspectors in analyzing results and focusing their oversight efforts on high-risk areas in air cargo security could be improved.

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.⁴⁷ We presented test cargo shipments to air carriers and certified cargo screening facilities, and the screeners or equipment did not always identify the test items.

Rail and Mass Transit

Passenger rail systems face a dynamic landscape of potential natural disasters, accidents, and terrorist attacks. Since 1995, there have been more than 250 terrorist attacks worldwide against rail targets, resulting in nearly 900 deaths and more than 6,000 injuries. Recent events on the rail and transit systems in Washington DC, including a derailment, fire, and crash, have raised questions regarding the mass transit agencies’ contingency plans and the ability to handle these basic issues, as well as major emergencies. The *Aviation and Transportation Security Act* assigned TSA the responsibility to secure all modes of transportation in the United States.

⁴⁶ DHS-OIG, *Security of Air Cargo During Ground Transportation*, (OIG-10-09, November 2009).

⁴⁷ DHS-OIG, *Evaluation of Screening of Air Cargo Transported on Passenger Aircraft*, (OIG-10-119, September 2010).

We evaluated the TSA's effectiveness in supporting mass transit and passenger rail agencies in preparing for and responding to emergency incidents.⁴⁸ As TSA expands its presence in non-aviation modes of transportation, it must look critically at how it is deploying resources. TSA could better support passenger rail agencies by improving its assessments of emergency preparedness and response capabilities. The agency could also improve its efforts to train passenger rail agencies and first responders, and ensure that drills and exercises are live and more realistic to help strengthen response capabilities. The agency has focused primarily on security and terrorism prevention efforts, while providing limited staff and resources to emergency preparedness and response.

TRADE OPERATIONS AND SECURITY

CBP is responsible for guarding nearly 7,000 miles of land border the United States shares with Canada and Mexico and 2,000 miles of coastal waters surrounding the Florida peninsula and off the coast of Southern California. The agency also protects 95,000 miles of maritime border in partnership with the United States Coast Guard. CBP assesses all people and cargo entering the U.S. from abroad for terrorist risk. Each year, more than 11 million maritime containers arrive at our seaports. At land borders, another 11 million arrive by truck and 2.7 million by rail. On a typical day CBP processes more than 50,000 truck, rail, and sea containers, along with the personnel associated with moving this cargo across U.S. borders or to U.S. seaports. To manage the potential security threats presented by this large volume of maritime cargo, CBP has implemented a layered approach to prevent cargo linked to terrorism from entering the country.

CBP uses several programs and initiatives including establishing voluntary cooperation and initiatives with government, industry and working with law enforcement and our foreign and domestic trade partners to improve international supply chain security. Among the programs and initiatives are the:

- Customs-Trade Partnership Against Terrorism (C-TPAT), a voluntary government-business initiative designed to improve international supply chain security by providing incentives to businesses that meet certain security standards.
- Container Security Initiative (CSI), an international program in which CBP officers are deployed at overseas ports to work with host nations to target containers that pose a high-risk. Currently, there are 58 CSI ports handling approximately 86% of all U.S. bound cargo.
- Secure Freight Initiative (SFI) a pilot program at foreign ports for testing the feasibility of scanning 100% of U.S. cargo.

⁴⁸ DHS-OIG, *TSA's Preparedness for Mass Transit and Passenger Rail Emergencies*, (OIG-10-68, March 2010).

- Importer Security Filing – CBP requires importers and carriers to submit additional cargo data on vessels destined to the U.S ports to help decision-makers and systems make more informed decisions on cargo.
- Automated Targeting System - CBP employs targeting and law enforcement tools and sophisticated targeting techniques to analyze and screen shipping information to identify the highest risk cargo on which to focus its limited resources.

While CBP continues to enhance its layered strategy, significant issues remain with modernizing trade systems, using resources efficiently, and managing and forging partnerships with foreign trade and customs organizations, and improving the effective use of its targeting systems.

For example, the targeting and examination of high risk shipments continues to be a challenge for CBP. Our most recent review highlighted several areas where improvement can be made. These areas include updating CBP's guidance relating to the physical examinations of high-risk cargo containers that may contain biological, chemical, nuclear, and radiological threats and the need for a risk assessment to determine which pathways, pose the highest risk.⁴⁹

As part of our review of CBP's layered approach, we evaluated the CSI program and noted that while the CSI program has proactive management and oversight processes in place, CSI could improve the future direction of the program by updating its performance measures and integrating its plans with other international maritime cargo security programs.⁵⁰

The challenge of developing and maintaining an integrated approach to cargo security is critical as CBP's moves forward to implement Section 1701 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, which requires DHS to screen all cargo headed for the United States that is loaded on or after July 1, 2012. Before 100% screening can be fully implemented for all cargo inbound to the U.S., DHS must ensure that it has adequate resources, infrastructure and processes in place and can 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.

⁴⁹ DHS-OIG, *CBP's Ability to Detect Biological and Chemical Threats in Maritime Cargo Containers*, (OIG-10-01, October 2009). DHS-OIG, *Cargo Targeting and Examinations*, (OIG-10-34, January 2010).

⁵⁰ DHS-OIG, *CBP's Container Security Initiative Has Proactive Management and Oversight but Future Direction is Uncertain*, (OIG-10-52, February 2010).

Appendix A

Report Distribution

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 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, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

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

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

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