



Department of Homeland Security Office of Inspector General

Major Management Challenges Facing the Department of Homeland Security



Office of Inspector General

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



**Homeland
Security**

November 12, 2008

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 2008 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.

It is our hope that 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

The creation of the Department of Homeland Security galvanized the Nation's fight against terrorism by consolidating and mobilizing the assets of the federal government under one roof with a single, focused mission: to ensure that the tragic events of Sept. 11, 2001, are never repeated again on American soil.

After just 5 short years, we are beginning to witness the positive effects of the department's efforts and initiatives: tighter security at the borders; increased immigration enforcement; greater cooperation with our international partners; expanded partnerships with the private sector; better and more efficient passenger screening at our airports; and regenerated disaster response and recovery management. Despite these considerable accomplishments, DHS still has much to do to establish a cohesive, efficient, and effective organization.

The major management challenges we have identified significantly affect the department's ability to protect our homeland and are decisive factors in setting priorities for audits, inspections, and evaluations of DHS programs and operations. As required by the *Reports Consolidation Act of 2000* (Public Law 106-531), we update our assessment of management challenges annually.

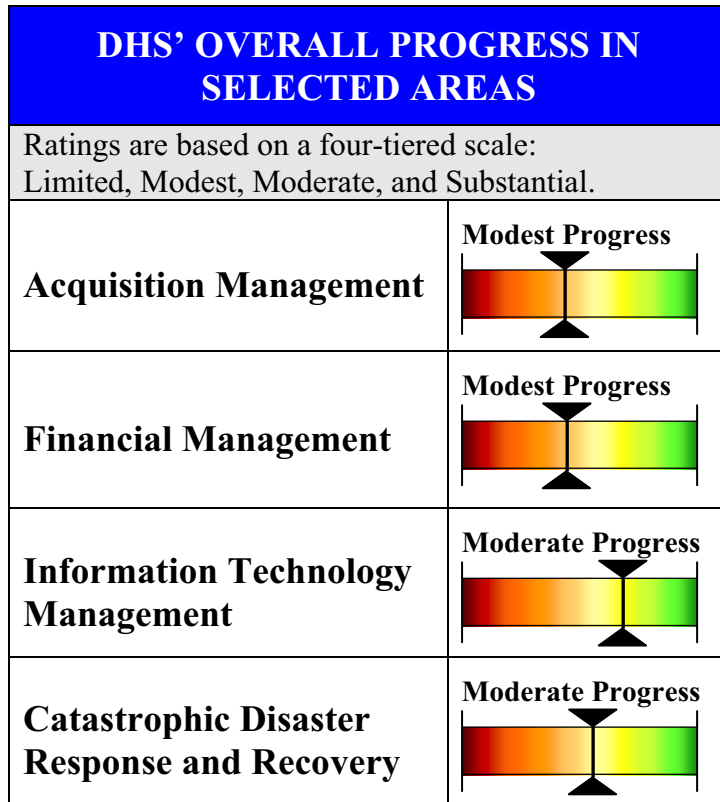
We have identified the following major management challenges:

- Acquisition Management
- Financial Management
- Information Technology Management
- Catastrophic Disaster Response and Recovery
- Grants 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 are developing scorecards to distinguish the department's progress in selected areas. Our

first scorecard, published in the *Semiannual Report to Congress*, October 1, 2006 – March 31, 2007, included an assessment of DHS’ acquisition function. This report features scorecards for acquisition management, financial management, information technology management, and catastrophic disaster response and recovery. These four scorecards are summarized in Figure 1 and incorporated in our discussion of the major management challenges.

Figure 1.



ACQUISITION MANAGEMENT

Contracting for goods and services consumes nearly 40% of the department’s annual budget and is absolutely critical to achieving its mission. Acquisition management is a complex process that goes beyond simply awarding a contract. It begins with the identification of a mission need; continues with the development of a strategy to fulfill that need while balancing cost, schedule, and performance; and concludes with contract closeout after the terms have been satisfactorily met. A successful acquisition process requires an effective acquisition management infrastructure.

The following are critical acquisition success 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 demonstrates areas where DHS has strengthened its acquisition management practices. We based our assessment on pertinent reports, particularly recent audit work conducted at the Federal Emergency Management Agency (FEMA), reports published by the Government Accountability Office (GAO), and congressional testimony. Given the scope of our review, we did not perform an in-depth assessment of each cornerstone of the acquisition framework. We used the critical elements within each—organizational alignment and leadership, policies and processes, acquisition workforce, and knowledge management and information systems—as well as our broader knowledge of the acquisition function, to gauge overall progress in those cornerstones.

The ratings were based on a four-tiered scale ranging from limited to substantial progress:

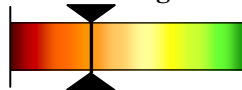
- **Limited:** While there may be plans to address critical success factors, few if any have been implemented;
- **Modest:** While some improvements have been made, many of the critical success factors have not yet been achieved;
- **Moderate:** Many of the critical success factors have been achieved;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

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

ACQUISITION MANAGEMENT SCORECARD

Organizational Alignment and Leadership

Modest Progress



DHS' executive leadership has made “modest” progress in ensuring that the acquisition program achieves the organizational alignment needed to perform its functions. The department continues to face challenges associated with implementing an acquisition function that is not fully integrated. According to GAO,¹ the structure of DHS' acquisition function creates ambiguity about who is accountable for acquisition decisions. The Chief Procurement Officer (CPO) has used collaboration and cooperation with the components as the primary means of managing DHS-wide acquisition oversight. However, the CPO faces challenges in implementing the corrective actions, as they are only recommendations, and the component head determines what action will be taken.²

FEMA has made “modest” progress in aligning the acquisition function to serve as a partner, rather than a support function, for FEMA program offices. The Office of Acquisition Management (OAM) has created an Acquisition Program & Planning branch, which aligns acquisition personnel with program functions and will serve as the primary link between acquisitions and the program areas that generate requirements.³ A major challenge is maintaining a sufficient acquisition workforce. In addition, OAM has experienced turnover of the senior leadership responsible for developing and communicating a strategic vision.

Policies and Processes

Modest Progress



DHS has made “modest” progress in developing policies and processes to ensure that components comply with regulations, policies, and processes to achieve department-wide goals. Previously, we reported that the department had begun implementation of its acquisition oversight plan, which incorporates DHS policy, internal controls, and elements of an effective acquisition function. However, the oversight program does not include an evaluation of outcomes from contracting methods such as performance-based acquisitions. According to GAO⁴, the initial implementation of the plan has helped the components prioritize actions to address identified weaknesses, although it is too early to assess the plan's overall effectiveness.

¹ GAO-07-948T, *Department of Homeland Security Ongoing Challenges in Creating an Effective Acquisition Organization*, June 2007.

² GAO-07-900, *Department of Homeland Security, Progress and Challenges in Implementing the Department's Acquisition Oversight Plan*, June 2007.

³ DHS-OIG, *FEMA's Preparedness for the Next Catastrophic Disaster*, OIG-08-34, March 2008.

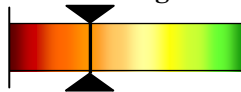
⁴ GAO-08-646T, *Progress Made in Implementation of Management Functions, But More Work Remains*, April 2008.

ACQUISITION MANAGEMENT SCORECARD

FEMA has implemented the Virtual Acquisition OfficeTM that provides an easily accessible, one-stop shop for useful acquisition guidance, and OAM has updated its *Emergency Acquisition Field Guide*. However, clear and transparent policies and processes for all acquisitions are still needed.

Acquisition Workforce

Modest Progress



DHS has made “modest” progress in building and maintaining a skilled acquisition workforce. Previously, we reported that personnel budget increases had allowed the department to fill many acquisition staff positions. However, there are still workforce challenges across the department. GAO reported in April 2008 that approximately 61% of the minimum required staff and 38% of the optimal level of contract specialists were in place. Components within the department such as the U.S. Coast Guard (Coast Guard) have initiatives to develop and retain a workforce capable of managing complex acquisition programs, but they are still relying on contractors to fill key positions. DHS also needs to improve the tracking of its acquisition workforce training and qualifications to ensure workforce development and appropriate assignment to acquisition projects.

FEMA has significantly increased the number of its acquisition staff and has developed training initiatives for them. However, FEMA needs to focus on preparing the acquisition workforce to respond to a catastrophic disaster.

Knowledge Management and Information Systems

Modest Progress



DHS has made “modest” progress in developing and deploying information systems to track and analyze acquisition data and improve user efficiency. Some progress has been made in the integration of information systems. For example, according to the Coast Guard, it has completed the integration of three separate Coast Guard accounting systems into a single Acquisition, Construction, and Improvement data set that is usable by all Coast Guard acquisition personnel as part of its Blueprint for Acquisition Reform. However, the department and its components still need to improve database reliability and verification.

FEMA has made limited progress in providing staff with the tools they need to carry out their jobs. The outdated and nonintegrated information systems currently used by acquisition personnel were to be replaced by the PRISM contract-writing system in early 2008. The PRISM roll-out has now been pushed back to 2009. Until PRISM is instituted, acquisition personnel must use nonintegrated systems that require duplicate

⁵ Statement of James L. Taylor, Deputy Inspector General, U.S. Department of Homeland Security, Before the Subcommittee on Management, Investigations, and Oversight, Committee on Homeland Security, U.S. House of Representatives, September 17, 2008; DHS-OIG, *Logistics Information Systems Need to be Strengthened at the Federal Emergency Management Agency*, OIG-08-60, May 2008.

ACQUISITION MANAGEMENT SCORECARD

input of data, thus increasing the possibility of errors. Logistics systems are not integrated with acquisition systems and do not provide complete asset visibility of disaster goods.⁵

FINANCIAL MANAGEMENT

DHS has continued to improve financial management in FY 2008, but challenges remain. As in previous years, our independent auditors were unable to provide an opinion on DHS' FY 2008 financial statements because the department could not provide sufficient evidence to support its financial statements or represent that financial statement balances were correct. The department has continued to remediate material weaknesses and has reduced the number of conditions that contribute to the disclaimer of opinion.

Although the Transportation Security Administration's (TSA) entity level controls deteriorated in FY 2008, the department made overall improvements in entity level controls at the departmental and component level. These improvements resulted in a reduction in the total number of material weaknesses from seven in FY 2007 to six in FY 2008. Even though new conditions were identified at FEMA and TSA, all components generally made progress in FY 2008.

As in FY 2007, the departmental material weaknesses in internal control were primarily attributable to the Coast Guard, FEMA, and TSA. The Coast Guard's material weaknesses, which have existed since 1994⁶, contribute to all six of the department's material weaknesses, while FEMA contributes to four and TSA contributes to three. The Coast Guard also contributes to TSA's financial systems security material weakness due to TSA's reliance on the Coast Guard's financial systems. Although the other components did not have material weaknesses, some had significant deficiencies that, when combined, contributed to the departmental material weaknesses.

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 2007. The scorecard is divided into two categories: (1) Military – Coast Guard and (2) Civilian – all other DHS components. The scorecard lists the seven material weaknesses and one other significant deficiency identified during the independent audit of the FY 2007 DHS consolidated balance sheet and statement of custodial activity. For a complete description of the internal control weaknesses identified in the FY 2007 audit, see OIG-08-12.⁷ To determine the status, we compared the

⁶ DOT-OIG, *Significant Internal Control Weaknesses Identified in Audits of FY 1994 and 1995*, R3-CG-6-011, August 1996.


⁷ DHS-OIG, *Independent Auditors' Report on DHS' FY 2007 Financial Statements*, OIG-08-12, November 2007.

material weaknesses reported by the independent auditor in FY 2007 with those reported in FY 2008. The scorecard does not include other financial reporting control deficiencies identified in FY 2008 that do not rise to the level of a significant deficiency, as defined by the American Institute of Certified Public Accountants. The ratings show that the department made some progress in FY 2008 toward remediation of the control weaknesses that were identified in FY 2007.


The ratings were based on a four-tiered scale ranging from limited to substantial progress as follows:

- **Limited:** While there may be plans to address internal control weaknesses, few if any have been remediated;
- **Modest:** While some improvements have been made, many of the internal control weaknesses have not yet been remediated;
- **Moderate:** Many of the internal control weaknesses have been remediated; and
- **Substantial:** Most or all of the internal control weaknesses have been remediated.

Based on the consolidated result of the seven financial management capability areas, DHS has made “modest” progress overall in the area of Financial Management.

FINANCIAL MANAGEMENT SCORECARD		
Financial Management and Entity Level Control: Entity level controls are the foundation that ensures internal control systems are comprehensively designed to achieve the mission and execute the department’s strategy.		
Military	Modest Progress	
	<p>The Coast Guard made “modest” progress in addressing its internal control weaknesses related to financial management and entity level controls. In FY 2007, the independent auditor’s report (IAR) noted that several conditions related to entity level control weakness also existed in prior years. For example, the Coast Guard did not fully implement a financial management organizational structure that incorporates U.S. generally accepted accounting principles or appropriately supports its financial statement balances. As a result, the Coast Guard could not assert to the completeness, existence (validity), accuracy, valuation, or presentation of its financial data.</p> <p>Although entity level control weaknesses continued to exist at the Coast Guard in FY 2008, some progress has been made. The FY 2008 IAR noted that the Coast Guard updated its Mission Action Plans in FY 2008 and created the <i>Financial Strategy for Transformation and Audit Remediation</i> (FSTAR). The FSTAR is a comprehensive plan to identify and correct the root causes of control deficiencies. However, most of the</p>	


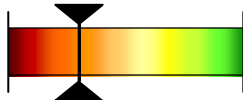
FINANCIAL MANAGEMENT SCORECARD

	<p>corrective actions outlined in the FSTAR were not scheduled to begin in FY 2008. Consequently, most of the entity level control weaknesses identified during FY 2007 continued to exist during FY 2008. The conditions noted at the Coast Guard contributed to an overall significant deficiency in entity level control at the department for FY 2008.</p>	
Civilian	Moderate Progress	
	<p>Overall, DHS has demonstrated “moderate” progress in establishing a financial management organization structure to enforce accountability and institute internal controls into the department’s culture. As a result, DHS has remediated the severity of this condition from a material weakness to a significant deficiency with Coast Guard, FEMA, and TSA contributing to this condition. However, while FEMA was the only civilian component that contributed to the material weakness in FY 2007, there is now one additional component (TSA) contributing to a significant deficiency in FY 2008.</p> <p>The department has undertaken and completed several steps designed to strengthen its entity and process level internal controls, thereby improving the reliability of financial reporting. These steps are documented in the DHS FY 2008 <i>Internal Control Playbook</i>, released in March 2008, and in component level Mission Action Plans finalized in FY 2008.</p> <p>During FY 2007, a number of internal control weaknesses related to financial management and entity level controls at FEMA rose to a material weakness at the DHS consolidated financial statement level. Among other conditions, the independent auditors noted that FEMA had not established a financial management organization structure with clear oversight and supervisory review functions that support the development and implementation of effective policies, procedures, and internal controls over financial reporting. Such policies, procedures, and controls are needed to ensure that accounting principles are correctly applied and accurate financial data is submitted to the Office of Financial Management for consolidation in a timely manner.</p> <p>FEMA has made “modest” progress toward correcting its entity level control deficiencies. During FY 2008, the independent auditors noted that FEMA developed Mission Action Plans to eliminate account balance qualifications identified in the IAR in FY 2007. However, some entity level control deficiencies identified in previous years continued to exist throughout FY 2008.</p>	

FINANCIAL MANAGEMENT SCORECARD

During FY 2008, TSA successfully addressed some account balance discrepancies and control deficiencies that contributed to the disclaimer of opinion on DHS' financial statements. However, during the FY 2008 audit, additional deficiencies that are indicative of weaknesses in entity level controls were identified at TSA.

Financial Reporting: Financial reporting is the process of presenting financial data about an agency's financial position, the agency's operating performance, and its flow of funds for an accounting period. The Federal Financial Management Improvement Act emphasizes the need for agencies to have systems that can generate timely, reliable, and useful information with which to make informed decisions to ensure ongoing accountability.

Military	Limited Progress	
	<p>The Coast Guard has demonstrated "limited" progress in remediating the numerous internal control weaknesses identified by the independent auditors during FY 2007. Significant control deficiencies contributing to a material weakness in financial reporting in FY 2007 included: 1) lack of an effective general ledger system; and 2) lack of effective policies, procedures, and controls surrounding the financial reporting process.</p> <p>Although the Coast Guard developed its FSTAR during FY 2008, most of the corrective actions outlined in the document are scheduled to occur after FY 2008. Consequently, the Coast Guard was unable to make substantial progress in correcting the control weaknesses that were reported in prior years, and a material weakness still existed in FY 2008.</p>	
Civilian	Modest Progress	
	<p>During FY 2008, DHS made "modest" progress in correcting the conditions that contributed to the material weakness in financial reporting in FY 2007. In FY 2007, conditions at the Office of Financial Management and FEMA rose to a level of material weakness, and conditions at TSA were considered a significant deficiency.</p> <p>During FY 2008, the Office of Financial Management fully corrected its material weakness over financial reporting, and FEMA made substantial progress toward correcting four material weaknesses that were reported in FY 2007. However, while FEMA has taken positive steps in FY 2008, some control weaknesses related to financial reporting continued to exist throughout FY 2008. These conditions at FEMA in the aggregate are considered a material weakness. In FY 2007, TSA adopted a two-year corrective action plan to address its financial reporting and other</p>	

FINANCIAL MANAGEMENT SCORECARD

accounting internal control weaknesses. This resulted in TSA making some progress in the development of its core accounting processes throughout FY 2008. However, the independent auditors noted additional and more serious financial reporting control weaknesses, some of which have existed since the agency's inception. As a result, the severity of the condition worsened in FY 2008 and TSA now has a material weakness condition in financial reporting at the department level.

Financial Systems Security: Financial systems security is essential to achieving effective, reliable reporting of financial and performance data.

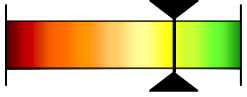

Military

Limited Progress





The Coast Guard has made “limited” progress in correcting certain information technology (IT) general control weaknesses identified in previous years. During FY 2007 significant control deficiencies included: 1) excessive access to key Coast Guard financial applications, 2) application change control processes that are not adequately designed nor operating effectively, 3) entity-wide security program issues involving personnel background checks, 4) system software weaknesses involving patch management, 5) segregation of duties involving lack of policies and procedures and excessive privilege access issues, and 6) service continuity issues involving the lack of disaster recovery testing . Significant deficiencies in application change control processes are among the principle causes of the Coast Guard's inability to support its financial statement balances. In addition, the Coast Guard was not able to effectively prioritize and implement Corrective Action Plans to remediate the root cause of the IT general control weaknesses in 2007. Many of these weaknesses were inherited from system development activities that did not incorporate strong security controls during the initial implementation of the system over five years ago, and will take several years to fully address. These weaknesses exist in the documentation of processes, the implementation of adequate security controls over processes, and within financial systems. In FY 2008, the Coast Guard remediated approximately 48% of its prior year IT general controls weaknesses. Specifically, the Coast Guard has made progress in remediation of issues in the areas of segregation of duties, systems software, and service continuity. Although there has been an improvement in the remediation effort, significant issues with the Coast Guard's change control process continue to exist for its financial applications.


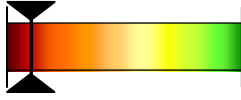
FINANCIAL MANAGEMENT SCORECARD

Civilian	Moderate Progress	
<p>The DHS Office of Chief Financial Officer and Office of Chief Information Officer (OCIO) have demonstrated moderate progress in improving their financial systems security. In FY 2007, two civilian components contributed to the financial systems security material weakness. Significant control deficiencies were noted in the areas of access controls, application change control and service continuity. In FY 2008, these two components continued to contribute to this material weakness although one component did make improvements in the area of service continuity. Overall improvements in the Federal Information System Controls Audit Manual domains for all civilian components resulted in the closing of approximately 43 % of the IT general control findings identified in FY 2007. One component however, continues to show significant weaknesses in the areas of access controls and application change controls for its financial systems. In addition, results of a performance audit conducted in FY 2008 noted that the OCIO's Plan of Action and Milestones process does not contain actionable steps to remediate the issues or address the root cause of the material weakness. In addition, Plans of Action and Milestones are not consistently updated, and there is no correlation between the OCIO's Plan of Action and Milestones and the Office of the Chief Financial Officer's OMB A-123 strategy.</p>		
<p>Fund Balance with Treasury (FBwT): FBwT represents accounts held at 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.</p>		
Military	Limited Progress	
<p>The Coast Guard has demonstrated "limited" progress in addressing the material weaknesses noted in this area in FY 2007. Some of the conditions noted in FY 2007 included: 1) lack of adequate supporting documentation that validated the accuracy of all of the Coast Guard FBwT reconciliations; 2) lack of an effective process for accounting for suspense account transactions related to FBwT; 3) the Coast Guard's inability to provide validated military and civilian payroll data to support payroll transactions processed through the Coast Guard's FBwT account.</p>		

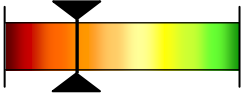

FINANCIAL MANAGEMENT SCORECARD

	<p>In FY 2008, the Coast Guard developed a remediation plan (FSTAR) to address the control deficiencies. However, most of the corrective actions noted in the plan are scheduled to occur after FY 2008, thus, many of the conditions identified in FY 2007 continued to exist throughout FY 2008. These control weaknesses at the Coast Guard resulted in an overall material weakness for the Department in FY 2008, as FBwT at the Coast Guard represented approximately 8.3 % of total DHS FBwT at the end of FY 2008.</p>	
Civilian	Substantial Progress	
	<p>No control deficiencies related to FBwT were noted at the civilian components in FY 2007. Corrective actions implemented in previous years continued to be effective throughout FY 2007 and FY 2008.</p>	
<p>Capital Assets and Supplies: 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 has demonstrated “limited” progress in remediating the control deficiencies related to capital assets and supplies in FY 2008. The Coast Guard maintains approximately 60% of all DHS’ property, plant, and equipment (PP&E), which includes a large fleet of boat and vessels. Since many of the Coast Guard’s assets are constructed over a multi-year period, have long useful lives, and undergo extensive routine servicing that may increase their value or extend their useful lives, comprehensive policies and procedures are necessary to accurately and timely account for these assets. In FY 2007, as in prior years, the independent auditors noted that the Coast Guard has been unable to provide auditable documentation for certain categories of PP&E due to a number of policy, control, and process deficiencies that will require several years to correct. Many of these conditions still existed throughout FY 2008.</p> <p>In FY 2008, the Coast Guard developed corrective action plans (FSTAR) to address the PP&E process and control deficiencies, and began remediation efforts. However, the corrective actions included in the FSTAR are scheduled to occur over a number of years. Consequently, most of the material weakness conditions cited in FY 2007 remained throughout FY 2008.</p>	

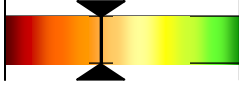
FINANCIAL MANAGEMENT SCORECARD

Civilian	Modest Progress	
	<p>Overall, the civilian components demonstrated “modest” progress in addressing the conditions identified in this area in FY 2007. In FY 2007, three civilian components contributed to a material weakness in capital assets and supplies. In FY 2007, conditions reported at FEMA rose to a level of material weakness, and significant deficiency at TSA and US-VISIT.</p> <p>During FY 2008, FEMA and US-VISIT were able to fully remediate the conditions leading to the material weaknesses identified in FY 2007. However, FEMA was unable to assert to the validity of internal use software and as a result, continues to contribute to the capital assets and supplies material weakness at the departmental level.</p> <p>Additionally in response to auditor inquiries, TSA initiated various reviews of its capital assets and identified errors in its accounting for equipment used in airports that required a number of restatements to the FY 2007 financial statement balances, and current year corrections. As a result, TSA was unable to assert to the validity of capital assets and supplies and contributes to the qualification of the financial statements and material weaknesses at the department level.</p> <p>Also, new control weaknesses were identified at Customs and Border Protection (CBP) which were considered a significant deficiency. CBP’s internal control deficiencies in this area are primarily related to construction of a fence along the border of the United States and Mexico. The FY 2008 IAR noted that CBP had expensed construction cost instead of capitalizing it as construction-in-progress.</p>	
<p>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, and legal and actuarial, and environmental liabilities.</p>		
Military	Limited Progress	
	<p>The Coast Guard maintains pension, medical, and postemployment 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>During FY 2008, the Coast Guard made “limited” progress in</p>	

FINANCIAL MANAGEMENT SCORECARD

	<p>remediating the conditions that contributed to the material weakness in this area. Control deficiencies identified by the independent auditors in FY 2007 and prior years continued to exist in FY 2008. For example, the FY 2008 IAR on DHS financial statements noted that the Coast Guard did not have effective policies, procedures, and controls to ensure the completeness and accuracy of participant, medical cost and other data provided to the actuary for the calculation of related benefit liabilities.</p>	
Civilian	Modest Progress	
	<p>Overall, the department demonstrated “modest” progress in this area. During FY 2008, TSA fully corrected the control weaknesses that contributed to a significant deficiency in this area in the prior year. Additionally, conditions at FEMA were reduced to significant deficiency (from material weakness in FY 2007). However, new control weaknesses that rise to the level significant deficiency were identified at three additional civilian components.</p> <p>For FY 2008, the auditors noted that FEMA had not established a reliable method to estimate certain accounts payable for accrual in the financial statements until the end of the fiscal year. Additionally, for FY 2008 the Federal Law Enforcement Training Center, Immigration and Customs Enforcement (ICE), and Science and Technology components did not fully implement policies and standard operating procedures that will allow management to assert that environmental liabilities have been recorded and disclosed in the financial statements in accordance with applicable accounting standards.</p> <p>In the aggregate, the significant deficiencies at the four components and the material weakness at the Coast Guard amount to an overall material weakness for the department.</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. Since the department received a disclaimer of opinion in FY 07, the audit is limited to the balance sheet and statement of custodial activity. As a result, audit coverage over budgetary accounts is limited to undelivered orders.</p>	
Military	Limited Progress	

FINANCIAL MANAGEMENT SCORECARD

	<p>The Coast Guard has made “limited” progress in this area. Many of the internal control weaknesses that contributed to a material weakness in budgetary accounting at the Coast Guard in FY 2007 remained throughout FY 2008. For example, the FY 2007 IAR 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 that recorded amounts are complete, valid, accurate, and that proper approvals and supporting documentation is maintained. This condition also existed during FY 2008. While some issues may take a number of years to be corrected, several of the budgetary control weaknesses can be corrected by process improvements and strengthened policies and internal controls.</p>	
Civilian	Modest Progress	
	<p>DHS has demonstrated “modest” progress in remediating internal control weaknesses that were noted in the FY 2007 IAR. During FY 2008, TSA corrected its material weakness in this area. However, DHS’ biggest challenge in this area remains at FEMA.</p> <p>In FY 2008, FEMA implemented corrective actions and performed an extensive review of its open obligations, including disaster relief and response mission assignments with other federal agencies. As a result, FEMA was able to deobligate over \$1 billion in funds prior to year-end, and make those funds available for FY 2008 disaster relief. FEMA also improved its processes and internal controls over the mission assignment obligation and monitoring process in FY 2008; however, significant control deficiencies remain. As a result, the departmental level material weakness condition remains at FEMA.</p> <p>Additionally, CBP did not enforce its policies and procedures to monitor and deobligate or closeout its obligations in a timely manner. In response to an audit inquiry, CBP initiated a review of open obligations and subsequently deobligated approximately \$84 million in open obligations in FY 2008. As a result, CBP has a significant deficiency condition related to budgetary accounting and contributes to the departmental level material weakness.</p>	

INFORMATION TECHNOLOGY MANAGEMENT

Creating a unified IT infrastructure for effective integration and agency-wide management of IT assets and programs remains a challenge for the DHS Chief Information Officer (CIO). In September 2008, we reported that DHS had taken steps to strengthen the CIO’s role for

centralized management of IT by providing greater authority and responsibility for overseeing component CIOs' IT acquisitions.⁸ As a result, the DHS CIO is better positioned to govern the department's IT investments and resources. However, continued CIO staffing shortages and inconsistent component-level IT budget practices hinder the DHS CIO's ability to fully integrate department-wide IT programs. We recommended that the DHS CIO update the CIO office's staffing plan, ensure that components submit comprehensive budgets, and develop and maintain IT strategic plans and enterprise architectures aligned with DHS' mission.

DHS also faces challenges in meeting OMB's requirement to transition to a new internet protocol, IPv6, which supports an unlimited number of IP addresses and other enhanced capabilities.⁹ Although DHS is in the early stages of the transition, the department is unlikely to be positioned to take timely advantage of the enhanced capabilities of IPv6. DHS must also ensure that several key activities, such as establishing a comprehensive inventory of all IPv6 devices, finalizing its IPv6 transition strategy, and engaging its components in IPv6 transition planning and activities, are completed before it can fully transition to IPv6 functionality.

Security of IT Infrastructure

During our FY 2007 *Federal Information Security Management Act*¹⁰ (FISMA) evaluation of the department's intelligence systems, we reported that much progress had been made in establishing an enterprise-wide IT security program that supports the department's intelligence operations and assets. However, procedural and operational issues remained regarding the implementation of the department's intelligence security program and system controls.¹¹

We also reviewed Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*. The purpose of HSPD-12 is to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors. The department is scheduled to complete its HSPD-12 implementation in 2010, two years after OMB's mandated deadline for all agencies.

In September 2008, we reported that components have not implemented appropriate security controls to enforce the department's policies on the acceptable use of portable storage devices.¹² The proliferation and uncontrolled use of portable storage devices (e.g., flash

⁸ DHS-OIG, *Progress Made in Strengthening DHS Information Technology Management, But Challenges Remain*, OIG-08-91, September 2008.

⁹ In August 2005 OMB issued Memorandum 05-22 (M-05-22), *Transition Planning for Internet Protocol Version 6 (IPv6)*, establishing the goal of transitioning federal agencies' wide area networks to IPv6.

¹⁰ Title III of the 2002 E-Government Act, Public Law 107-347

¹¹ DHS-OIG, *Challenges Remain in Executing the Department of Homeland Security's Information Technology Program for Its Intelligence Systems*, OIG-08-48, April 2008.

¹² DHS-OIG, *Review of DHS Security Program for Portable Storage Devices*, OIG-08-95, September 2008.

drives, external hard drives, and portable music players) increases the risk of theft and mishandling of sensitive information.

DHS Component IT Management

Although improvements have been made, DHS continues to struggle with agency-wide IT management, planning, and investment, which has resulted in limited system integration and data sharing. For example, in October 2007, we reported that due to a lack of authority and standard policies to govern technology implementation, TSA's CIO faces significant challenges in conducting agency-wide IT planning and investment management. We concluded that TSA's IT management could be strengthened by empowering the CIO with IT budget authority, developing an agency-wide strategic planning approach, implementing an enterprise architecture, establishing guidelines to manage IT development, and increasing staff resources within the IT division.

Similarly, our April 2008 assessment of FEMA's efforts to upgrade its disaster logistics management systems¹³ showed that, although the agency has made short-term progress in addressing disaster goods procurement and delivery during disasters, more remains to be done to address long-term planning and systems integration needs. FEMA has taken steps to improve its logistics capabilities by gathering independent evaluations to assess its existing systems, identify IT systems requirements, and select technologies to meet its logistics needs. However, existing systems do not provide complete asset visibility, comprehensive asset management, or integrated logistics information. We recommended that FEMA finalize its logistics strategy and operational plans, develop standard business processes and procedures for logistics activities, evaluate current technologies, and develop a strategy for acquiring IT systems to support the logistics mission.

Privacy

DHS still faces challenges in ensuring that privacy concerns are addressed throughout the lifecycle of each program and information system that contains sensitive personally identifiable information. According to the *E-Government Act of 2002*, federal agencies must conduct a Privacy Impact Assessment (PIA) for each new or substantially changed IT system that collects, uses, maintains, or disseminates personally identifiable information, demonstrating that they have incorporated privacy safeguards throughout the development lifecycle of their programs or systems. Although DHS requires PIAs at the very earliest stage of a project or before beginning a pilot test, DHS officials did not conduct risk assessments in a number of IT system implementations.¹⁴

In April 2008, we reported that the Intelligence and Analysis' National Applications Office (NAO) had made progress by involving the DHS Privacy Office early in its privacy program planning and development of key organizational documents. However, a revised PIA and a

¹³ DHS-OIG, *Logistics Information Systems Need to be Strengthened at the Federal Emergency Management Agency*, OIG-08-60, May 2008.

¹⁴ DHS Privacy Office, *Privacy Impact Assessment Guidance*, May 2007.

Civil Liberties Impact Assessment reflecting changes in NAO’s Charter and proposed operations were also necessary before NAO become operational.¹⁵

IT Management Scorecard

The following scorecard demonstrates where IT management functions of the DHS CIO and the seven largest DHS component-level CIO offices 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. The ratings were based on a four-tiered scale ranging from limited to substantial progress:

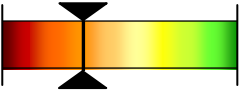
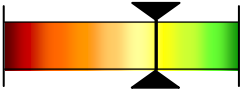
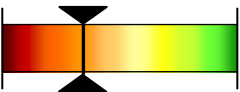
- **Limited:** Plans are in place for this capability, but the capability has not been fully implemented;
- **Modest:** The capability is partially implemented, with limited IT management benefits realized;
- **Moderate:** The capability is implemented with moderate IT management benefits realized; and
- **Substantial:** The capability is implemented with substantial IT management benefits realized.

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

IT MANAGEMENT SCORECARD		
IT Budget Oversight: ensures visibility into IT spending and alignment with the strategic IT direction.		
DHS CIO	Modest Progress	
	<p>The DHS CIO has made improvements in managing department-wide IT budgets in accordance with the <i>Clinger-Cohen Act</i> and the department’s mission and policy guidance. The DHS CIO plans to conduct reviews across the department of all investments that contain IT assets and services. The goals for IT budget reviews are to resolve IT budget issues prior to OMB submission, align IT investments with targets and priorities, and eliminate redundancies. Progress in this area was further evidenced by the FY 2010 IT budget planning guidance, issued in January 2008, on better integrating component IT resource reviews with DHS program and budget reviews. With support of DHS leadership, the</p>	

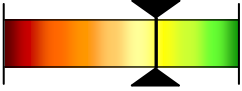
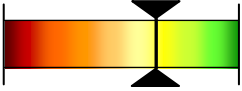
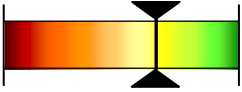
¹⁵ DHS-OIG, *National Applications Office Privacy Stewardship*, OIG-08-35, April 2008.

IT MANAGEMENT SCORECARD

	DHS OCIO will continue to focus on improving IT budget capabilities.	
Component CIOs	Modest Progress	
	<p>Overall, components demonstrated “modest” progress in conducting IT budget planning and programming functions. Although component-level IT budget responsibilities have increased through <i>DHS Management Directive</i> 0007.1, more than 70% of DHS component CIOs remain hindered by ineffective, decentralized IT budget practices. Most component CIOs plan to further centralize existing IT budget functions to meet requirements in the management directive to prepare a component IT budget. A number of DHS components are implementing initiatives to increase centralized management of IT investments by restructuring and consolidating IT spending accounts that are currently managed by separate offices throughout the agency.</p>	
IT Strategic Planning: helps align the IT organization to support mission and business priorities.		
DHS CIO	Moderate Progress	
	<p>Per OMB Circular A-130, 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. The DHS OCIO has made progress aligning IT with department goals. Although the current IT strategic planning approach does not fully link technology to mission requirements, the OCIO plans to achieve strategic outcomes and stronger IT alignment with the Secretary’s goals. The OCIO is currently updating DHS’ IT strategic plan and has communicated the plan’s goals to the CIO Council.</p>	
Component CIOs	Modest Progress	
	<p>As of January 2008, approximately 70% of the component-level CIOs had developed an IT strategic plan as required by <i>Management Directive</i> 0007.1. However, not all components can consistently link strategic goals and objectives with IT investments. Further, although some component CIOs said that they had developed an IT strategic plan, not all are up-to-date.</p> <p>Improvements are planned by some component CIOs who are updating their IT strategic plans. However, until the improvements are made, the agency may fall short of its potential to improve business processes and systems.</p>	

IT MANAGEMENT SCORECARD

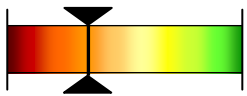
Enterprise Architecture: functions as a blueprint to guide IT investments for the organization.

DHS CIO	Moderate Progress	
	<p>The <i>Clinger-Cohen Act</i>¹⁶ 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-level enterprise architecture has advanced greatly as an effective tool for reviews and IT management decision-making. Overall, the DHS OCIO has increased its ability to enforce architecture alignment through <i>Management Directive 0007.1</i>. Significant progress is due in part to the IT Acquisition Review process, which has helped promote and enforce such alignment. The OCIO plans to mature and optimize the department’s architecture through performance-based outcomes and to develop the data architecture further in mission-critical areas.</p>	
Component CIOs	Moderate Progress	
	<p><i>Management Directive 0007.1</i> requires component CIOs to implement a detailed enterprise architecture specific to the component’s mission and in support of DHS’ mission. As of January 2008, more than 70% of the component-level CIOs could align IT investments with the department’s architecture. Most components have component-level architectures used for some degree of IT investment decision-making. However, architecture products, such as reference models, definitions of current and future state architectures, and transition plans are in varying stages of development or use. A number of components said that their architecture products were out of date or needed to be better defined.</p>	
<p>Portfolio Management: improves leadership’s ability to understand interrelationships between IT investments and department priorities and goals.</p>		
DHS CIO	Moderate Progress	
	<p>The DHS OCIO has made “moderate” progress in establishing the department’s portfolio management capabilities as instructed by OMB Circular A-130.¹⁷ The DHS portfolio management program aims to</p>	

¹⁶ *Clinger-Cohen Act of 1996*, Public Law 104-106, Division E, Section 5125, February 10, 1996.

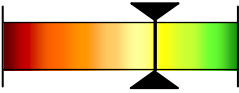
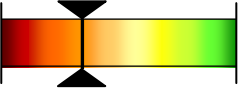
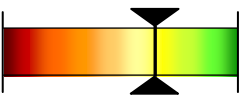
¹⁷ Revision of Office of Management and Budget Circular A-130, Transmittal 4, *Management of Federal Information Resources*, July 1994.

IT MANAGEMENT SCORECARD

	<p>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 organizational boundaries.</p> <p>The DHS OCIO has a solid plan in place to implement portfolio management capabilities in FY 2008. The OCIO has recently finalized plans, along with the first round of documentation and guidance, for a department-level portfolio management approach. Currently, there are 22 defined portfolio areas, six of which are considered priority areas: infrastructure, geospatial, case management, human resources, screening and credentialing, and finance. In addition, OCIO has created a portfolio management integrated project team to develop transition plans, measure performance, and standardize the portfolio management process. Although progress is being made, the department is not yet realizing management benefits from the portfolio management program. As a result, the department may miss opportunities for system integration and cost savings.</p>	
Component CIOs	Modest Progress	
	<p>Overall, DHS components have made “modest” progress in establishing portfolio management capabilities. Full implementation of this capability remains a work in progress, due in part to challenges in creating and aligning component-specific portfolios with DHS’ 22 portfolios. Most DHS component-level CIOs have developed a mapping approach to align component IT systems with DHS-level portfolios.</p> <p>Many CIOs said that it is a complicated process to align their unique mission and business processes with multiple DHS-level IT portfolios. For example, Coast Guard officials said that they are working with DHS OCIO officials to determine which portfolios will be associated with each of the systems they identified in the IT budget review. Until this capability is fully implemented, DHS components may continue to invest in systems within organizational silos, limiting opportunities for consolidation and cost savings.</p>	

IT MANAGEMENT SCORECARD

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

DHS CIO	Moderate Progress	
<p>The <i>Clinger-Cohen Act</i> 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. Through such efforts, in FY 2007, the 94 DHS programs on the management watch list were reduced to 18. In FY 2008, 53 programs are listed. Officials in the OCIO have sought to remove these programs from the list by working with the program managers through the CPIC Administrator’s bimonthly meetings.</p>		
Component CIOs	Modest Progress	
<p>Most components have not yet achieved an integrated planning and investment management capability. More than 70% of the major DHS components had limited capital planning processes outside the existing OMB 300 process. However, some component CIOs said that they are creating a CPIC process to integrate with existing governance structures such as the Investment Review Board. For example, the ICE Investment Review Board resembles a CPIC group, incorporating major areas such as security, budget, and enterprise architecture. The ICE CIO said that this process has helped components leverage resources more effectively.</p>		
<p>IT Security: ensures protection that is commensurate with the harm that would result from unauthorized access to information.</p>		
DHS CIO	Moderate Progress	
<p>DHS IT security is rated at “moderate,” for progress made during the last 2 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. The DHS CIO has taken an active role in ensuring that components comply with FISMA. In 2007, the CIO requested that components focus on improving areas such as certification and accreditation, annual self-</p>		

IT MANAGEMENT SCORECARD

	assessments, and plan of action and milestones management. According to the DHS OCIO, additional quality control measures have been implemented manage the certification and accreditation process better. The DHS OCIO also plans to focus on improving disaster recovery and continuity of operations over the coming year.
	(Components were not rated on IT Security)

CATASTROPHIC DISASTER RESPONSE AND RECOVERY

The primary mission of FEMA is to reduce the loss of life and property and protect the Nation from all hazards, including natural disasters, acts of terrorism, and other man-made disasters. FEMA does this by leading and supporting the Nation in a risk-based, comprehensive emergency management system of preparedness, protection, 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.¹⁸ FEMA made moderate progress in five of the nine areas: overall planning, coordination and support, interoperable communications, logistics, and acquisition management. FEMA made modest progress in evacuation, housing, and disaster workforce, and limited progress in mission assignments. (Please see the catastrophic disaster response and recovery scorecard below for a discussion of selected areas.) Our broader recommendations addressed the improvements needed in overall planning, coordination, and communications. FEMA officials said that budget shortfalls, reorganizations, inadequate IT systems, and confusing or limited authorities impeded their progress.

In FY 2009, we will continue to conduct studies regarding FEMA’s preparedness, response, and recovery efforts. These studies will allow us to further assess FEMA’s progress in transforming itself to be better prepared to lead the federal effort in responding to a catastrophic disaster.

Catastrophic Disaster Response and Recovery Scorecard

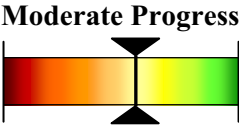
The following scorecard highlights FEMA’s progress in six key areas: logistics, evacuations, housing, disaster workforce, mission assignments, and acquisition management. The ratings were based on a four-tiered scale ranging from limited to substantial progress:

- **Limited:** There is an awareness of the critical issues needing to be addressed, but specific corrective actions have not been identified;
- **Modest:** corrective actions have been identified, but implementation is not yet underway;

¹⁸ DHS-OIG, *FEMA’s Preparedness for the Next Catastrophic Disaster*, OIG-08-34, March 2008.

- **Moderate:** Implementation of corrective action is underway, but few if any have been completed; and
- **Substantial:** Most or all of the corrective actions have been implemented.

Based on the consolidated result of the six areas, FEMA has made “moderate” progress in the area of catastrophic disaster response and recovery.

FEMA CATASTROPHIC DISASTER RESPONSE AND RECOVERY SCORECARD	
Logistics	<p>Moderate Progress</p> 
<p>The mission of FEMA’s Logistics Management Directorate is to plan, manage, and sustain the national logistics response and recovery operations in support of domestic emergencies. FEMA has made “moderate” progress in meeting its logistics responsibilities such as acquiring, receiving, storing, shipping, tracking, sustaining, and recovering commodities, assets, and property in the event of a catastrophic disaster.</p> <p>The <i>Post-Katrina Emergency Management Reform Act of 2006 (Post-Katrina Act)</i>¹⁹ requires FEMA to develop a logistics system that provides visibility of disaster goods from procurement to delivery. FEMA has not yet met this requirement. FEMA’s total asset visibility system is unable to track goods from warehouses to staging areas to distribution sites. Nor can it track goods received from federal and nonfederal partners. FEMA needs to finalize its logistics plans, implement standardized processes and procedures for logistics activities, and develop a strategy for acquiring IT systems to support the logistics mission.²⁰</p> <p>Determining the types and quantities of commodities that FEMA may need in the aftermath of a disaster is a continuing challenge. In 2005, FEMA was criticized for having too few commodities available in the aftermath of Hurricane Katrina. In 2006, FEMA acquired inventory that was not needed during the mild hurricane season, resulting in waste. In-depth analysis of this issue resulted in FEMA’s determination that pre-positioning commodities is neither logistically prudent nor an effective use of taxpayer funds. Instead, FEMA plans to rely on public and private sector partners to provide needed items. FEMA appears to have made progress in developing these partnerships, as well as working more closely with states to determine where state shortfalls are likely to occur.</p> <p>A Distribution Management Strategy Working Group is developing and documenting an integrated national policy and strategy for managing and controlling inventory,</p>	

¹⁹ Public Law 109-295, Title VI – National Emergency Management, *Department of Homeland Security Appropriations Act of 2007*.

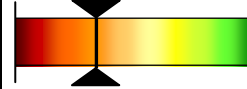
²⁰ DHS-OIG, *Logistics Information Systems Need to Be Strengthened at the Federal Emergency Management Agency*, OIG-08-60, May 2008.

FEMA CATASTROPHIC DISASTER RESPONSE AND RECOVERY SCORECARD

positioning commodities, and distributing critical resources. In the past, FEMA has been prone to drafting strategies, policies, and procedures that were never finalized. FEMA leadership should ensure that this Working Group proposes strategies and policies in a timely manner and that these proposals are promptly reviewed, finalized, and implemented.

Evacuations

Modest Progress

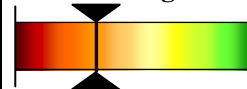


The conduct of evacuation operations is generally a state, tribal, and local responsibility. However, some circumstances exceed the capabilities of those jurisdictions to support mass evacuations. Where federal support is required, FEMA coordinates the support with the affected state, local and tribal governments. Federal support is scaled to the incident level and may be provided in the form of cost reimbursement or direct assistance, for example, providing buses, trains, and air ambulances for evacuation.

FEMA has a number of initiatives underway for improving evacuation management capabilities and published a *Mass Evacuation Incident Annex* describing evacuation functions and agency roles and responsibilities in mass evacuations. However, no single entity within FEMA is responsible for emergency evacuation planning or operations. FEMA has not yet developed a single national system to support multistate, state-managed, or local evacuation operations. Coordinating transportation for evacuees during emergencies, collaborating with states to receive and accommodate the needs of evacuees, and ensuring that dedicated resources are available to support evacuation plans, remain significant challenges.

Housing

Modest Progress



Although improvements have been made, disaster housing remains a major challenge, as demonstrated by the results of our recent audits of FEMA housing programs and initiatives. Issues with accountability, management, and disposal of emergency housing units persist. Plans for addressing catastrophic disaster housing needs must be developed and tested. As we have learned from past and recent disasters, not being prepared with a full range of housing options has significant implications for evacuees and the states and communities that host them.

In March 2008, we reported that FEMA had made modest progress in the key preparedness area of housing. While FEMA is striving to improve its disaster housing assistance strategy and coordination, it needs to develop and test innovative catastrophic disaster housing plans to deal with large-scale displacement of citizens for extended periods, where traditional housing programs have been shown to be inefficient, ineffective, and costly.

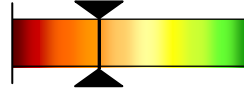
FEMA CATASTROPHIC DISASTER RESPONSE AND RECOVERY SCORECARD

In October 2008, we reported that FEMA’s strategy for ending its direct housing assistance program is generally sound, and that FEMA has made considerable progress recovering temporary housing units in the Gulf Coast region.²¹ However, FEMA’s strategy is not complete since FEMA’s strategy has not recertified resident eligibility or taken action to recover temporary housing units from ineligible residents. FEMA must implement the recertification of eligibility process to ensure recovery of all temporary housing units by March 1, 2009, which is the ending date of FEMA’s direct housing assistance program for hurricanes Katrina and Rita.

The *Post-Katrina Act* requires FEMA to develop, coordinate, and maintain a National Disaster Housing Strategy (NDHS). FEMA released the draft NDHS for a 60-day public comment period in July 2008. We are currently conducting a review of FEMA’s future housing strategies and are reviewing the NDHS as part of this effort. FEMA must move forward with a finalized strategy to guide future disaster housing efforts.

Disaster Workforce

Modest Progress



A trained, effective disaster workforce is one of the most effective tools FEMA has to meet its mission. FEMA’s disaster workforce consists mainly of reservists who serve temporarily during a disaster, with no employee benefits. During the 2005 Gulf Coast hurricanes, FEMA struggled to provide qualified staff and did not have the automated support to deploy more than 5,000 disaster personnel on short notice. As FEMA evolves, its disaster workforce strategy, structure, and systems need to keep pace.

To date, FEMA has not completed or has not been able to verify the completion of five of nine workforce-related actions required by the *Post-Katrina Act*. The five incomplete or unconfirmed actions are:

- Developing a Strategic Human Capital Plan;
- Establishing career paths;
- Conferring with state, local, and tribal government officials when selecting regional administrators;
- Training regional strike teams as a unit and equipping and staffing these teams; and
- Implementing a surge force capacity plan.

The congressionally mandated due dates for these actions range from March 2007 through July 2007.

²¹ DHS-OIG, *FEMA’s Exit Strategy for Temporary Housing in the Gulf Coast Region*, OIG-09-02, October 2008.

FEMA CATASTROPHIC DISASTER RESPONSE AND RECOVERY SCORECARD

Mission Assignments

Limited Progress



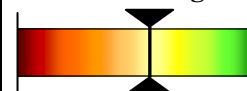
FEMA is responsible for coordinating the urgent, short-term emergency deployment of federal resources to address immediate threats and for stewardship of the associated expenditures from the Disaster Relief Fund. FEMA uses mission assignments to request disaster response support from other federal agencies. Past audits and reviews regarding mission assignments have concluded that FEMA’s management controls were generally not adequate to ensure that:

- Deliverables (missions tasked) met requirements;
- Costs were reasonable;
- Invoices were accurate;
- Federal property and equipment were adequately accounted for or managed; and
- FEMA’s interests were protected.

FEMA guidelines regarding the mission assignment process, from issuance of an assignment through execution and closeout, have never been fully developed, creating misunderstandings among federal agencies concerning mission assignment operational and fiduciary responsibilities. Implementing Section 693 of the *Post-Katrina Act*, which allows FEMA to designate up to 1% of the funds provided to federal agencies for disaster relief activities as oversight funds, will help ensure effective stewardship and oversight of monies the recipient agencies use for activities conducted under the FEMA reimbursable mission assignment process.

Acquisition Management (Catastrophic Disasters)

Moderate Progress



After a disaster, FEMA’s tendency has been to acquire goods and services quickly, but with insufficient attention to costs, definition of requirements, and competition. To balance urgency of needs with good business practices, FEMA’s OAM has awarded approximately 27 pre-disaster response contracts and 70 recovery contracts. Planning and negotiating these contracts in advance of a disaster provides more advantageous terms to the government and more opportunity for small and local businesses.

FEMA has found it difficult to recruit experienced acquisition staff. FEMA has increased its acquisition staff from just 35 when Hurricane Katrina struck to about 150 today. FEMA has also increased staffing and training of contracting officer’s technical representatives (COTRs), who are responsible for technical contract oversight, inspecting goods, and approving invoices. However, staffing remains a challenge. The new acquisition personnel need training and experience in acquiring goods and services under emergency circumstances. Recent OIG reports recommended increased oversight of contractor actions and reviews of services and invoices by COTRs.

FEMA CATASTROPHIC DISASTER RESPONSE AND RECOVERY SCORECARD

FEMA needs to continue hiring and training acquisition personnel, allocating staff where the need is greatest among Headquarters and the 10 FEMA regional offices, and developing reliable, integrated financial and information systems.

GRANTS MANAGEMENT

Monitoring and documenting the effectiveness of DHS' multitude of grant programs poses an increasingly significant challenge for the department. DHS manages more than 80 disaster and non-disaster grant programs. This challenge is compounded by other federal agencies' grant programs that assist state and local governments in improving their abilities to prepare for, respond to, and recover from acts of terrorism or natural disasters. FEMA has yet to fully implement the April 2007 reorganization directed by the *Post Katrina Emergency Management Reform Act of 2006*. Most states are not sufficiently monitoring subgrantee compliance with grant terms and cannot clearly document critical improvements in preparedness as a result of grant awards.

During FY 2008, we issued audit reports on homeland security preparedness grant management by the states of New Jersey, Ohio, Michigan, Georgia, Florida, Utah, Arizona, and Washington. These states generally did an adequate job of administering the program requirements; however, the most prevalent areas needing improvement concerned the monitoring of subgrantees and controls over personal property and equipment.

We are concluding audits of the effectiveness of grant awards under the State Homeland Security Grant Program in California and Illinois. During the first quarter of FY 2009, we also anticipate issuing an audit mandated by the *Implementing Recommendations of the 9/11 Commission Act of 2007* (Public Law 110-53) on FEMA's grant management and oversight practices.

Given the billions of dollars appropriated annually for preparedness, disaster, and non-disaster grant programs, DHS needs to ensure that internal controls are in place and adhered to, and that grant recipients are sufficiently monitored to achieve successful outcomes. DHS should continue refining its risk-based approach to awarding preparedness grants to ensure that areas and assets that represent the greatest vulnerability to the public are as secure as possible. Sound risk management principles and methodologies will help DHS prepare for, respond to, recover from, and mitigate acts of terrorism and natural disasters.

INFRASTRUCTURE PROTECTION

DHS has direct responsibility for leading, integrating, and coordinating efforts to protect 10 critical infrastructure and key resources (CI/KR) sectors: the chemical industry; commercial

facilities; 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.²² 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 FY 2007, we reported several opportunities for DHS to improve its engagement of public and private partners and to prioritize resources and activities based on risk.²³ For example, a comprehensive national database that inventories assets is essential to provide a comprehensive picture of the Nation's CI/KR and to enable management and resource allocation decision-making. We are reviewing how DHS uses an asset database to support its risk management framework. We also plan to evaluate how DHS coordinates infrastructure protection with other sectors by reviewing the protection of petroleum and natural gas infrastructure within the energy sector.

Protecting national as well as internal cyber infrastructure continues to be a challenge for DHS. We recently reviewed the department's progress in identifying and prioritizing its internal cyber critical infrastructure in accordance with Homeland Security Presidential Directive 7.²⁴ This directive established a national policy for the federal government to identify, prioritize, and protect U.S. critical infrastructure, including the internal critical assets used by each department. We found that the department needs to take additional steps to produce a prioritized inventory and to coordinate related efforts to secure these assets. We recommend that the department assign responsibility and provide the resources necessary to determine protection priorities for its internal critical infrastructure, including critical cyber infrastructure. In addition, the department should develop a process to coordinate internal efforts to protect these assets. In FY 2009, we plan to review the National Cyber Security Division's strategy for control systems security and its Computer Emergency Readiness Team.

BORDER SECURITY

A principal DHS challenge is reducing America's vulnerability to terrorism by controlling the borders of the United States. To this end, DHS is implementing the Secure Border Initiative (SBI), a comprehensive multi-year program to secure the borders and reduce illegal immigration. The Coast Guard, U.S. Citizenship and Immigration Services, CBP, and ICE

²² 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.

²³ DHS OIG, *A Review of Homeland Security Activities Along a Segment of the Michigan-Canadian Border*, OIG-07-68, August 2007; *Review of the Buffer Zone Protection Program*, OIG-07-59, July 2007; *The Department of Homeland Security's Role in Food Defense and Critical Infrastructure Protection*, OIG-07-33, February 2007.

²⁴ DHS OIG, *Letter Report: DHS Needs to Prioritize Its Cyber Assets*, OIG-08-31, March 2008.

all have key roles in the SBI program. To ensure SBI success, it is critical that the program be thoroughly planned. DHS also must institute an approach to coordinating the SBI functions and activities of the participating DHS components with the related efforts of other agencies. We are conducting a series of audits to evaluate whether the SBI program initiatives are being accomplished in an economical, efficient, and effective manner.

The technology component of SBI, known as *SBI_{net}*, involves the acquisition, development, integration, and deployment of surveillance systems. It also involves communications and intelligence technologies. In FY 2006, we recommended that CBP improve the effectiveness of remote surveillance technology to correct the lack of integration between border surveillance cameras and ground sensors, which were plagued by false alarms.²⁵ CBP has made some progress in improving surveillance and detection technology along the Southwest border via Project 28, which includes enhanced radars, sensors, and cameras. However, delays associated with software integration problems have required CBP to extend the completion dates for implementation from December 2008 to sometime in 2009. Consequently, Border Patrol Agents continue to use technology that predates *SBI_{net}* and, in the Tucson, Arizona sector, they are still using capabilities from *SBI_{net}*'s prototype system despite previously reported performance shortfalls.²⁶

The definition and management of requirements is another significant challenge for the *SBI_{net}* program. According to GAO,²⁷ the *SBI_{net}* program office issued guidance on the development and acquisition of software and systems that is consistent with recognized leading practices. However, this guidance was not finalized until February 2008, and thus was not used in performing a number of important requirements-related activities. For example, there is a lack of traceability among the different levels of requirements. This limits the program office's ability to determine whether the scope of the contractor's design, development, and testing efforts will produce a system that meets operational needs and performs as intended.

Also, efforts are needed to ensure that ICE can support its detention and removal operations. In our recent reviews of ICE's oversight of immigration detention facilities, we recommended that ICE improve its standards, strengthen its oversight of facilities, and enhance operations.²⁸ We are completing an audit of ICE's acquisition and management of "bed space" needs to support detention and removal operations.

²⁵ DHS-OIG, *A Review of Remote Surveillance Technology along U.S. Land Borders*, OIG-06-15, December 2005.

²⁶ GAO-08-1141T, *SBI Observations on Deployment Challenges*, September 2008.

²⁷ GAO-08-1086, *Secure Border Initiative: DHS Needs to Address Significant Risks in Delivering Key Technology Investment*, September 2008.

²⁸ DHS-OIG, *ICE Policies Related to Detainee Deaths and the Oversight of Immigration Detention Facilities*, OIG-08-52, June 2008; DHS-OIG, *ICE's Compliance with Detention Limits for Aliens with Final Order for Removal from the U.S.*, OIG-07-28, February 2007; DHS-OIG, *U.S. Immigration and Customs Enforcement's Detainee Tracking Process*, OIG-07-08, November 2006; DHS-OIG, *Treatment of Immigration Detainees Housed at Immigration and Customs Enforcement Facilities*, OIG-07-01, December 2006; *Detention and Removal of Illegal Aliens*, OIG-06-33, April 2006.

TRANSPORTATION SECURITY

The Nation's transportation system, which moves millions of passengers and tons of freight every day, is an attractive terrorist target and creates an enormous security challenge due to its size and complexity. TSA was originally created as a part of the Department of Transportation after September 11, 2001, to strengthen the security of the Nation's transportation systems, including aircraft, ships, rail, motor vehicles, airports, seaports, transshipment facilities, roads, railways, bridges, and pipelines. However, since its inception, TSA has focused on aviation.

Checkpoint and Checked Baggage Performance

The *Aviation and Transportation Security Act*²⁹ requires TSA to screen or inspect all passengers, goods, and property before entry into the sterile areas of an airport. Our undercover audits of screener performance revealed that improvements are needed in the screening process to ensure that dangerous prohibited items are not carried into the sterile areas of heavily used airports and do not enter the checked baggage system. In past testing, we noted four areas that caused most of the test failures: training; equipment and technology; policies and procedures; and management and supervision. TSA agreed with our conclusion that significant improvements in screener performance will be possible only with the introduction of new technology. TSA plans to purchase 300 advanced technology x-rays and 80 passenger imagers. Currently TSA has 700 advanced x-rays and 40 passenger-imaging units deployed at 12 airports. We recently released a classified report on our penetration testing results, specifically at those airports with explosives trace portals and an airport that had a whole body imager, and found that improvements to effectively secure sterile airport areas are still needed.³⁰

The OIG will continue to exercise oversight of TSA's performance and processes of checkpoint and checked baggage screening. We are currently in the process of conducting audits of TSA's controls over screener uniforms, badges, and identification cards, as well as the effectiveness of TSA's explosives detection systems on-screen alarm resolution protocol. These reports will be issued later this year.

Employee Workplace Issues

A stable, mature, and experienced TSA workforce is one of the most effective tools to meet the agency's mission. Despite the value of the TSA workforce, employees have expressed their concerns about how the agency operates by historically filing formal complaints at rates higher than other federal agencies of comparable size. Our audit of TSA's efforts to address employee concerns found that low employee morale continues to be an issue at some airports and has contributed to TSA's 17% voluntary attrition rate.³¹

²⁹ Public Law 107-71, November 19, 2001.

³⁰ DHS-OIG, *Airport Passenger and Checked Baggage Performance*, OIG-08-25, February 2008.

³¹ DHS-OIG, *TSA's Efforts to Proactively Address Employee Concerns*, OIG-08-62, May 2008.

More than half the employees we interviewed described the agency's efforts to educate them on the various initiatives available to address their workplace concerns as "inadequate." We made six recommendations to the Assistant Secretary of TSA to provide employees with sufficient tools, including clear guidance and better communication, on the structures, authorities, and oversight responsibilities of the initiatives we reviewed. TSA fully or partly concurred with five of the recommendations and has taken action to resolve them.

Passenger Air Cargo Security

The vast and multifaceted U.S. air cargo system transports approximately 7,500 tons of cargo on passenger planes each day, making air cargo vulnerable to terrorist threats. 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. We are conducting an audit to assess how TSA ensures that cargo from unknown shippers is not being shipped on passenger planes. This report is expected to be issued later this year. During 2009, we also plan to audit TSA's cargo security measures during ground movement.

Rail and Mass Transit

Since the terrorist attacks of September 11, 2001, the London subway bombings, and the Madrid rail bombings, DHS has taken steps to manage risk and strengthen our Nation's rail and transit systems. While most mass transit systems in this country are owned and operated by state and local government or private industry, securing these systems is a shared responsibility among federal, state, and local partners.

DHS operates multiple programs, including several grants, to improve rail and mass transit security. In June 2008, we reported on TSA's efforts to secure mass transit through four major assistance programs: the Surface Transportation Security Inspection Program, Transit Security Grant Program, Visible Intermodal Prevention and Response program, and the deployment of canine explosive detection teams for rail.³² TSA needs to clarify its transit rail mission, improve interoffice communication and coordination, develop memorandums of understanding with local transit authorities, and develop additional regulations. TSA also needs to understand and address system-specific security requirements better. We are completing mandates to review the effectiveness of the Trucking Industry Security Grant Program and to report further on the Surface Transportation Security Inspection Program.

During emergencies transit agencies must rely on well-designed and regularly practiced drills and exercises to respond and recover rapidly and effectively. Recent events on the rail systems in Washington DC, including a derailment and a fire, have raised questions regarding the mass transit agencies' contingency plans and the ability to handle these basic issues, as well as major emergencies. We will evaluate TSA's efforts to ensure that mass transit agencies are prepared to respond and recover from emergencies on passenger rail systems. We will review TSA's role in security program management and accountability,

³² DHS-OIG, *TSA's Administration and Coordination of Mass Transit Security Programs*, OIG-08-66, June 2008.

security and emergency response training, drills and exercises, public awareness, and other protective measures for passenger rail systems.

TRADE OPERATIONS AND SECURITY

CBP is primarily responsible for trade operations and security, with the support of the Coast Guard and ICE. Each year, more than 16 million containers arrive in the United States by ship, truck, and rail. CBP typically processes more than 70,000 truck, rail, and sea containers per day, along with the personnel associated with moving this cargo across U.S. borders or to U.S. seaports. Modernizing trade systems, using resources efficiently, and managing and forging partnerships with foreign trade and customs organizations pose significant challenges for CBP and DHS.

CBP works with trade representatives to implement processes and systems to help secure the supply chain and uses targeting systems to identify the highest risk cargo on which to focus its limited resources. Recently, CBP increased its international efforts to secure the cargo supply chain by expanding its work with the Customs-Trade Partnership against Terrorism program and by improving its multi-layered security strategy.

The *Coast Guard and Maritime Transportation Act of 2004* (Public Law 108-293) requires us to evaluate and report annually on the effectiveness of the Automated Targeting System (ATS), which is an intranet-based enforcement and decision support tool used by CBP seaport inspectors to help determine which containers entering the country will undergo inspection. Our annual ATS review in 2008³³ focused on a subsystem of ATS, the Cargo Enforcement Reporting and Tracking System (CERTS), which is designed to gather data on cargo examination findings and report on how efficiently examination equipment is being used. We identified the need for improvements in planning, updating, developing, and implementing CERTS. Specifically, CBP needs to update the project plan to include the scope of work, and a detailed implementation schedule for system design, developing and testing, and cost estimates past phase one. In addition, CBP bypassed key life cycle reviews designed to ensure that end users have a properly working system and have received management's approval to continue the project.

The Coast Guard is responsible for developing and implementing a comprehensive National Maritime Transportation Security Plan to deter and respond to transportation security incidents. Our most recent annual review of mission performance³⁴ revealed that the Coast Guard must make several improvements to implement the *Maritime Transportation Security Act of 2002* (Public Law 107-295) in a timely and effective manner. For example, the Coast Guard needs to balance the resources devoted to the performance of homeland and non-homeland security missions; improve the performance of its homeland security missions; maintain and re-capitalize its Deepwater fleet of aircraft, cutters, and small boats; restore the

³³ DHS-OIG, *Targeting of Cargo Containers 2008: Review of CBP's Cargo Enforcement Reporting and Tracking System*, OIG-08-65, June 2008.

³⁴ DHS-OIG, *Annual Review of Mission Performance – FY2006*, OIG-08-30, February 2008.

readiness of small boat stations to perform their search and rescue missions; and increase the number and quality of resource hours devoted to non-homeland security missions.

We are reviewing CBP's Account Management Program and National Targeting and Analysis Groups, which aim to improve revenue collection compliance. We are also reviewing DHS' planning, management oversight, and implementation of security measures to protect against small vessel threats.

Appendix A

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Executive Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Under Secretary Management
Assistant Secretary for Public Affairs
Assistant Secretary for Policy
Assistant Secretary for Legislative Affairs
Chief Financial Officer
Chief Information Officer
Chief Security Officer
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Program 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) 254-4199, 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.