



# 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**

NOV 13 2009

### 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 2009 assessment of the major management challenges facing the Department of Homeland Security. As required by the *Reports Consolidation Act of 2000* (Public Law 106-531), we update our assessment of management challenges annually.

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

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

Richard L. Skinner  
Inspector General



Homeland  
Security

## Major Management Challenges Facing the Department of Homeland Security

The creation of the Department of Homeland Security (DHS) on March 1, 2003, was the most significant reorganization of the federal government bringing together twenty-two federal agencies in response to the aftermath of 9/11. Since its inception, the Department of Homeland Security performs a broad range of activities across a single driving mission to secure America from the entire range of threats that we face.

Six years later, the department is moving beyond operating as an organization in transition to a department diligently working to protect our borders and critical infrastructure, preventing dangerous people and goods from entering our country, and recovering from natural disasters effectively. However, while much progress has been done, the department still has much to do to establish a cohesive, efficient, and effective organization.

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

We have identified the following major management challenges:

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

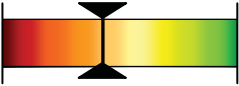
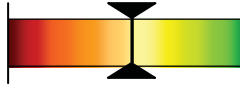
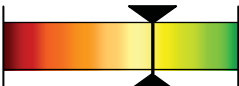


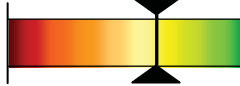
Since the major management challenges have tended to remain the same from year to year, we developed scorecards to distinguish the department’s progress in selected areas. Our first scorecard, published in the *Semiannual Report to Congress*, October 1, 2006 – March 31, 2007, included an assessment of DHS’ acquisition function. This report features scorecards for acquisition management, information technology management, emergency management, grants management, and financial management.

We based the ratings on a four-tiered scale ranging from limited to substantial progress<sup>1</sup>:




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

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

**Figure 1.**

<b>DHS’ OVERALL PROGRESS IN SELECTED AREAS</b>		
Ratings are based on a four-tiered scale: Limited, Modest, Moderate, and Substantial.		
	FY 2008	FY 2009
<b>Acquisition Management</b>	<b>Modest Progress</b> 	<b>Moderate Progress</b> 
<b>Information Technology Management</b>	<b>Moderate Progress</b> 	<b>Moderate Progress</b> 
<b>Emergency Management</b>	<b>Moderate Progress</b> 	<b>Moderate Progress</b> 

<sup>1</sup> Financial Management Scorecard uses different criteria to assess limited to substantial progress, and is shown in the Financial Management section of the report.

<b>DHS' OVERALL PROGRESS IN SELECTED AREAS</b>		
Ratings are based on a four-tiered scale: Limited, Modest, Moderate, and Substantial.		
	FY 2008	FY 2009
<b>Grants Management</b>	N/A	<b>Modest Progress</b> 
<b>Financial Management</b>	<b>Modest Progress</b> 	<b>Modest Progress</b> 

## **ACQUISITION MANAGEMENT**

DHS relies on goods and services contractors to help fulfill many of its critical mission areas. As such, effective acquisition management is vital to achieving DHS' overall mission. Acquisition management is much more than simply awarding a contract. It requires a sound management infrastructure to identify mission needs; develop strategies to fulfill those needs while balancing cost, schedule, and performance; and ensure that contract terms are satisfactorily met. A successful acquisition process depends on the following key factors:

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

### **Acquisition Management Scorecard**

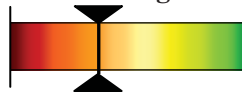
The following scorecard illustrates areas where DHS improved its acquisition management practices, as well as areas where it continues to face challenges. We based our assessment on our recent audit reports, Government Accountability Office (GAO) reports, congressional testimony, and our broader knowledge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

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

## ACQUISITION MANAGEMENT SCORECARD

### Organizational Alignment and Leadership

**Modest Progress**



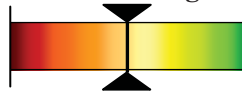
DHS made “modest” progress in improving the acquisition program’s organizational alignment and defining roles and responsibilities. The department continues to depend on a system of dual accountability and collaboration between the chief procurement officer and the component heads, which may sometimes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

According to the Government Accountability Office (GAO),<sup>2</sup> DHS has not effectively implemented or adhered to its investment review process, which requires executive decision making at key points in an investment’s life cycle. DHS has not provided the oversight needed to identify and address cost, schedule, and performance problems in its major investments due to a lack of involvement by senior management officials as well as limited monitoring and resources.

Although FEMA has reorganized its acquisition function to operate strategically,<sup>3</sup> FEMA program offices have not adequately integrated the acquisition function into their decision-making activities. Planning strategically requires that the Acquisition Management Division partner with other FEMA components and assist them in assessing internal requirements and the impact of external events. FEMA’s Acquisition Management Division has begun to work more closely with program offices to better manage the acquisition process, monitor and provide oversight to achieve desired outcomes, and employ knowledge-based acquisition approaches.

### Policies and Processes

**Moderate Progress**



DHS made “moderate” progress in developing and strengthening its policies and processes related to acquisition management. Although the department has put a great

<sup>2</sup> GAO-09-29, *Department of Homeland Security: Billions Invested in Major Programs Lack Appropriate Oversight*, November 2008.

<sup>3</sup> DHS-OIG, *FEMA's Implementation of Best Practices in the Acquisition Process*, (OIG-09-31, February 2009).

## ACQUISITION MANAGEMENT SCORECARD

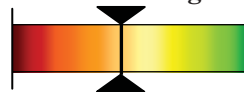
deal of effort into improving its processes and controls over awarding, managing, and monitoring contract funds, it still needs to do more.

According to a May 2009 report by the GAO,<sup>4</sup> DHS provided guidance on award fees<sup>5</sup> in its acquisition manual, but individual contracting offices developed their own approaches to executing award fee contracts that were not always consistent with the principles in the Office of Management and Budget's guidance on award fees or among offices within DHS. In addition, DHS has not developed methods for evaluating the effectiveness of an award fee as a tool for improving contractor performance. FEMA also needs to accelerate its planned acquisition process improvements for awarding, managing, monitoring, tracking, and closing-out contracts.<sup>6</sup>

DHS is making progress in the oversight of its services contracts. As of March 2009, all DHS professional services contracts greater than \$1 million will undergo a mandatory review before a new contract is awarded or an existing contract is renewed to ensure that proposed contract awards do not include inherently governmental functions or impact core functions that must be performed by federal employees. DHS expects this additional review to add a new level of rigor to the DHS contracting process.

### Acquisition Workforce

**Moderate Progress**



DHS made “moderate” progress in recruiting and retaining a workforce capable of managing a complex acquisition program, but continues to face workforce challenges across the department. An April 2009 report by the GAO indicated that the Coast Guard filled 717 of its 855 military and civilian personnel positions in the acquisition branch<sup>7</sup> and planned to expand its acquisition workforce in FY 2011. However, some of its unfilled positions are core acquisition positions such as contracting officers and specialists, program management support staff, and engineering and technical specialists. Although FEMA has improved acquisition training and greatly increased the number of acquisition staff, it still needs to better prepare its acquisition workforce for catastrophic disasters.<sup>8</sup>

<sup>4</sup> GAO-09-630, *Federal Contracting: Guidance on Award Fees Has Led to Better Practices but is Not Consistently Applied*, May 2009.

<sup>5</sup> An award fee is an amount of money that a contractor may earn in whole or in part by meeting or exceeding subjective criteria stated in an award fee plan.

<sup>6</sup> DHS-OIG, *Internal Controls in the FEMA Disaster Acquisition Process*, (OIG-09-32, February 2009); DHS-OIG, *Challenges Facing FEMA's Disaster Contract Management*, (OIG-09-70, May 2009); DHS-OIG, *FEMA's Acquisition of Two Warehouses to Support Hurricane Katrina Response Operations*, (OIG-09-77, June 2009); DHS-OIG, *FEMA's Temporary Housing Unit Program and Storage Site Management*, (OIG-09-85, June 2009).

<sup>7</sup> GAO-09-620T, *Coast Guard: Update on Deepwater Program Management, Cost, and Acquisition Workforce*, April 2009.

<sup>8</sup> DHS-OIG, *Challenges Facing FEMA's Acquisition Workforce*, (OIG-09-11, November 2008).

## ACQUISITION MANAGEMENT SCORECARD

In its response to our November 2008 management challenges report, DHS highlighted headquarters-level initiatives for building and retaining its acquisition workforce<sup>9</sup>. For example, DHS centralized recruitment and hiring of acquisition personnel, established the Acquisition Professional Career Program to hire and mentor procurement interns, created a tuition assistance program, and structured rotational and development work assignments. However, DHS needs time to complete all of these new initiatives. In the interim, personnel shortages will continue to hamper the department's ability to manage its contracts and workload in an effective and efficient manner.

### Knowledge Management and Information Systems

Modest Progress



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

In recent years, DHS did not ensure contract data was complete and accurate in the Federal Procurement Data System-Next Generation (FPDS-NG).<sup>10</sup> This system is the only consolidated information source for analyzing competition on procurements and is relied on for reporting to the public and Congress. DHS has taken steps to comply with May 2008 guidance, issued by the Office of the Federal Procurement Policy, that requires government agencies to develop a plan for improving the quality of acquisition data entered into FPDS-NG. For example, DHS developed a standard report format and data quality review plans.

## INFORMATION TECHNOLOGY MANAGEMENT

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

<sup>9</sup> *Department of Homeland Security FY 2008 Annual Financial Report.*

<sup>10</sup> DHS-OIG, *DHS Contracts Awarded Through Other Than Full and Open Competition during Fiscal Year 2007*, (OIG-09-94, August 2009).

## Security of IT Infrastructure

During our FY 2008 *Federal Information Security Management Act*<sup>11</sup> (FISMA) evaluation, we reported that the department continued to improve and strengthen its security program. Specifically, the department implemented a performance plan to improve on four key areas: Plan of Action and Milestones weaknesses remediation, quality of certification and accreditation, annual testing and validation, and security program oversight. The department also finalized its Sensitive Compartmented Information Systems Information Assurance Handbook, which provides department intelligence personnel with security procedures and requirements to administer its intelligence systems and the information processed.

Although the department's efforts have resulted in some improvements, components are still not executing all of the department's policies, procedures, and practices. Management oversight of the components' implementation of the department's policies and procedures needs improvement in order for the department to ensure that all information security weaknesses are tracked and remediated, and to enhance the quality of system certification and accreditation.

Additional information security program areas that need improvement include configuration management, incident detection and analysis, specialized training, and privacy. In 2009, we reported<sup>12</sup> that DHS had implemented effective system controls to protect the information stored and processed by the department's unclassified network, LAN-A. DHS ensures that network patch management and vulnerability assessments are performed periodically. However, DHS did not have an effective process to manage its LAN-A privileged accounts or ensure that security patches were deployed on all applications. The lack of sufficient processes increased the risk that LAN-A security controls could be circumvented.

## IT Management

The department faces significant challenges as it attempts to create a unified IT infrastructure for effective integration and agency-wide management of IT assets and programs. Toward that end, DHS has several initiatives underway to improve IT operations and reduce costs. One such program is the development of an enterprise-wide IT disaster recovery program to ensure that the department's operations can continue uninterrupted should its IT systems fail. We reported in April 2009 that DHS had made progress in implementing a disaster recovery program by allocating funds to establish two new data centers.<sup>13</sup> However, we noted that more work was needed to ensure the new data centers were fully capable of meeting the department's significant IT disaster recovery needs.

Another major IT challenge for the DHS CIO is OneNet, an initiative aimed at consolidating existing IT infrastructures into a wide area network. DHS began work on OneNet in 2005, and envisions it will provide the components with secure data, voice, video, tactical radio,

---

<sup>11</sup> Title III of the E-Government Act of 2002, Public Law 107-347.

<sup>12</sup> DHS-OIG, *Better Monitoring and Enhanced Technical Controls Are Needed to Effectively Manage LAN-A*, (OIG-09-55, April 2009).

<sup>13</sup> DHS-OIG, *DHS' Progress In Disaster Recovery Planning for Information Systems* (OIG-09-60, April 2009).

and satellite communications between internal and external DHS resources. We reported in September 2009 that DHS has taken various steps to consolidate existing infrastructures into OneNet, but faces challenges in completing its OneNet implementation.<sup>14</sup> Specifically, we reported that DHS is experiencing delays in meeting its scheduled completion date and that components are reluctant to participate and are not subscribing to the implementation of OneNet. As a result, DHS may not be able to reach its ultimate goal of consolidating and modernizing its existing infrastructures and achieve cost savings.

Component CIOs also face significant challenges in their efforts to improve IT management, budgeting, planning, and investment. In July 2009, we reported<sup>15</sup> that U.S. Citizenship and Immigration Services (USCIS) strengthened overall IT management by restructuring its Office of Information Technology and realigning its field IT staff. However, the department's efforts to enforce overall IT budget authority and improve agency-wide IT infrastructure have been difficult, due to insufficient staffing and funding. The department finalized its Office of the Chief Information Officer (OCIO) Staffing Plan in April 2009, in which it has identified the need to ensure sufficient staff with the right skills, security clearances and experience.

Our April 2008 audit of the Federal Emergency Management Agency's (FEMA) efforts to upgrade its disaster logistics management systems<sup>16</sup> showed that existing systems did not provide complete asset visibility, comprehensive asset management, or integrated logistics information. Since this report, FEMA has yet to finalize its logistic, strategic, and operational plans to guide logistics activities. In addition, FEMA has not developed processes and procedures to standardize logistics activities. Without such plans, processes, and procedures, selection of IT systems to support logistics activities will remain difficult.

## **Privacy**

DHS continues to face challenges in ensuring that privacy concerns are properly addressed throughout the lifecycle of each program and information system. For example, our September 2009 report<sup>17</sup> identified a need for automated privacy tools to monitor the Transportation Security Administration's (TSA) file servers containing personally identifiable information. Without such tools, TSA's OCIO manually checked for personally identifiable information leaks on file servers. However, these manual checks did not prevent regularly occurring classified data spills and unprotected e-mails containing personnel information.

We also reported that TSA made progress in implementing a framework that promotes a privacy culture and complies with federal privacy laws and regulations. Specifically, TSA designated the Office of Privacy Policy and Compliance to oversee its privacy functions.

---

<sup>14</sup> DHS-OIG, *Improved Management and Stronger Leadership are Essential to Complete the OneNet Implementation* (OIG-09-98, September 2009).

<sup>15</sup> DHS-OIG, *U.S. Citizenship and Immigration Services' Progress in Modernizing Information Technology* (OIG-09-90, July 2009).

<sup>16</sup> DHS-OIG, *Logistics Information Systems Need to be Strengthened at the Federal Emergency Management Agency*, (OIG-08-60, May 2008).

<sup>17</sup> DHS-OIG, *Transportation Security Administration Privacy Stewardship* (OIG-09-97, August 2009).






















the FY 2009 independent auditor’s report. For a complete description of the internal control weaknesses identified in the FY 2008 audit, see OIG-09-09.<sup>32</sup> To determine the status, we compared the material weaknesses reported by the independent auditor in FY 2008 with those identified in FY 2009.<sup>33</sup> The scorecard does not include other financial reporting control deficiencies identified in FY 2009 that do not rise to the level of a material weakness, as defined by the American Institute of Certified Public Accountants.

The ratings are 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 and account balances have been corrected, many systemic internal control weaknesses remain;
- **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 areas included in the report, DHS has made “**modest**” progress overall in financial management.

FINANCIAL MANAGEMENT SCORECARD		
<p><b>Financial Reporting and Management:</b> Financial reporting is the process of presenting financial data about an agency’s financial position, the agency’s operating performance, and its flow of funds for an accounting period. Financial management is the planning, directing, monitoring, organizing, and controlling of financial resources, including program analysis and evaluation, budget formulation, execution, accounting, reporting, internal controls, financial systems, grant oversight, bank cards, travel policy, appropriation-related Congressional issues and reporting, working capital funds, and other related functions.</p>		
Military	<b>Limited Progress</b>	
	<p>The Coast Guard has demonstrated limited progress in remediating the numerous internal control weaknesses identified by the independent auditors during FY 2008. Significant control deficiencies contributing to a material weakness in financial reporting in FY 2008 included: 1) lack of an effective general ledger system; and 2) lack of effective policies, procedures, and controls surrounding the financial reporting process. In</p>	

<sup>32</sup> DHS-OIG, *Independent Auditors’ Report on DHS’ FY 2008 Financial Statements*, (OIG-09-09, November 2008).

<sup>33</sup> DHS-OIG, *Independent Auditors’ Report on DHS’ FY 2009 Financial Statements and Internal Control Over Financial Reporting*, (OIG-10-11, November 2009).



## FINANCIAL MANAGEMENT SCORECARD

	<p>FY 2008 the Coast Guard revised its FSTAR; however, most of the actions outlined in the FSTAR were scheduled to occur after FY 2008.</p> <p>During FY 2009, the independent auditors noted that the Coast Guard continued implementation of its FSTAR and made some progress by completing its planned corrective actions over pension liabilities. This allowed management to make assertions on completeness and accuracy on its accrued liabilities, which represents more than 50 percent of the department's total liabilities. However, most corrective actions outlined in the FSTAR are scheduled to occur after FY 2009, and consequently many of the financial reporting weaknesses reported in prior years remained as of the end of FY 09.</p> <p>Among the conditions at Coast Guard that contribute to a material weakness in this area during FY 2009 is the lack of sufficient financial management personnel to identify and address control weaknesses, and develop and implement effective policies, procedures, and internal controls over financial reporting process.</p>	
<b>Civilian</b>	<b>Limited Progress</b>	
	<p>FY 2008, the independent auditors found several internal control weaknesses in financial reporting at FEMA and TSA. Those conditions contributed to qualifications of the auditors' opinion on the department's consolidated financial statements.</p> <p>Overall, the department has made limited progress in FY 2009 in addressing the internal controls weakness the auditor identified in this financial reporting in FY 2008. FEMA and TSA, which both contributed to a material weakness in this area in FY 2008, have shown only minimal progress in improving the internal control weaknesses. Conditions at CBP have deteriorated in FY 2009, although less severe than at FEMA and TSA. These internal control deficiencies at CBP, FEMA, and TSA have contributed to a material weakness in this area for the department overall in FY 2009.</p> <p>Among the deficiencies noted in the FY 2009 independent auditor's report is that the department lacks a sufficient number of accounting and financial management personnel with core technical competencies to ensure its financial statements are prepared accurately and in compliance with generally accepted accounting principles. This condition was common among CBP, FEMA, and TSA in FY 2009.</p>	

## FINANCIAL MANAGEMENT SCORECARD

### Information Technology Controls and Financial Systems Functionality:

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

Military	<b>Limited Progress</b>	
	<p>During 2008, the independent auditors identified numerous IT general control deficiencies, of which nearly all were repeat findings from prior years. The most significant IT deficiencies that could affect the reliability of the financials statements related to the development, implementation, and tracking of scripts, and the design and implementation of configuration management policies and procedures. These deficiencies at the Coast Guard contributed to a material weakness for the department in this area in FY 2008.</p> <p>For FY 2009, the Coast Guard has demonstrated limited progress in correcting certain IT general control weaknesses identified in previous years. As a result of the increase in scope of IT testing in FY 2009, the auditors have identified additional weaknesses that were not reported in the prior year. Therefore, although the Coast Guard corrected some deficiencies in IT general controls, the number of IT control weaknesses increased over the prior year. Over 50 percent of the findings the auditors identified in FY 2009 were repeat conditions from the prior year.</p> <p>One key area that remains a challenge for the Coast Guard is its core financial system configuration management process. For 2009, the auditors again noted that the configuration management process is not operating effectively. Financial data in the general ledger may be compromised by automated and manual changes that are not properly controlled. The changes are implemented through the use of IT script process, which was instituted as a solution to address functionality and data quality issues. However, the controls over the script process were not properly designed or implemented effectively from the beginning.</p>	
Civilian	<b>Limited Progress</b>	
	<p>Overall, DHS has made limited progress in correcting the IT general and applications control weaknesses identified in the FY 2008 independent auditor's report. During FY 2008, FEMA and TSA contributed to an overall material weakness in IT general and applications control, while CBP, FLETC, and USCIS all had significant deficiencies in this area.</p>	


## FINANCIAL MANAGEMENT SCORECARD



As a result of the increase in scope of the IT testing in FY 2009, the auditors have identified additional weaknesses that were not reported in the prior year. Therefore, although the DHS civilian components corrected some deficiencies in IT general controls, which resulted in the closure of more than 60 percent of the IT general controls findings reported in FY 2008, the number of department-wide IT control weaknesses increased over the prior year, with conditions at FEMA and ICE deteriorating.

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

The FY 2009 independent auditor's report identified the following areas that continue to present risks to the confidentiality, integrity, and availability of DHS' financial data: 1) excessive access to key DHS financial applications, 2) application change control processes that are inappropriate, not fully defined or followed, and are ineffective, and 3) security management practices that do not fully and effectively ensure that financial systems are certified, accredited, and authorized to operation prior to implementation.

**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.

<b>Military</b>	<b>Limited Progress</b>	
	<p>The Coast Guard has demonstrated limited progress in addressing the material weaknesses noted in this area in previous years. In FY 2008, the independent auditors reported a material weakness in internal control over FBwT at the Coast Guard. During FY 2009, the Coast Guard corrected some of the control deficiencies related to this area and revised its remediation plan (FSTAR) to include additional corrective actions, which are scheduled to occur after FY 2009. Consequently, most of the conditions which existed in FY 2008 continued to exist throughout FY 2009. For example, the auditors reported that the Coast Guard has not</p>	

FINANCIAL MANAGEMENT SCORECARD		
	developed a comprehensive process, to include effective internal controls, to ensure that all FBwT transactions are recorded in the general ledger timely, completely, and accurately.	
Civilian	N/A	
	No control deficiencies related to FBwT were identified at the civilian components in FY 2009. Corrective actions implemented in previous years continued to be effective throughout FY 2008 and FY 2009.	
<p><b>Property, Plant, and Equipment (PP&amp;E) and Operating Materials and Supplies (OM&amp;S):</b> 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	<b>Limited Progress</b>	
	<p>The Coast Guard maintains approximately 52 percent of the department's property, plant, and equipment (PP&amp;E), including a large fleet of boats and vessels. In FY 2008, internal control weaknesses related to PP&amp;E at Coast Guard contributed to a material weaknesses in this area for the department.</p> <p>For FY 2009, the Coast Guard has demonstrated limited progress overall in correcting internal control weaknesses related to PP&amp;E identified in the independent auditor's report in FY 2008.</p> <p>During FY 2009, the Coast Guard continued implementation of its remediation plan (FSTAR) to address the PP&amp;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 reported in FY 2008 remained throughout FY 2009. For example, one of the conditions the auditors identified, which is a repeat from prior years, is that the Coast Guard has not established its beginning PP&amp;E balance necessary to prepare the year-end balance sheet.</p> <p>The auditors also identified weaknesses related to operating materials and supplies (OM&amp;S), which the Coast Guard maintains in significant quantities. These consist of tangible personal property to be consumed in normal operation to service marine equipment, aircraft, and other equipment. The auditors reported that the Coast Guard has not</p>	

**FINANCIAL MANAGEMENT SCORECARD**

implemented policies, procedures, and internal controls to support financial assertions related to OM&S and related balances for FY 2009.

Civilian	<b>Modest Progress</b>	
----------	------------------------	--

DHS has demonstrated modest progress overall in correcting internal control weaknesses related to capital assets and supplies identified in the independent auditor’s report in FY 2008. In FY 2008, FEMA, TSA, and CBP contributed to a material weakness in capital assets and supplies. The conditions that existed at TSA and FEMA prevented the auditors from completing their test work in FY 2008 and led to qualifications in the auditors’ report.

While FEMA has fully remediated its internal control weakness in this area during FY 2009, internal control conditions have deteriorated at CBP, USCIS, ICE, and NPPD. Although conditions at USCIS, ICE, and NPPD appear less severe than at CBP and TSA, when taken together, they contribute to an overall material weakness for the department in this area for FY 2009.

Most of the control weakness conditions in this area are related to PP&E. Common among the components that contributed to the material weakness is the lack of adequate accounting policies, procedures, processes, and controls to properly account for its PP&E.

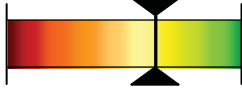

**Actuarial and Other Liabilities:** Liabilities represent the probable and measurable future outflow or other sacrifice of resources as a result of past transactions or events. The internal control weaknesses reported in this area are related to various types of liabilities, including accounts and grants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

Military	<b>Limited Progress</b>	
----------	-------------------------	--

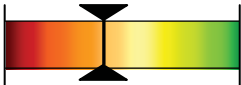
The Coast Guard maintains medical and post-employment travel benefit programs that require actuarial computations to record related liabilities for financial reporting purposes. Other liabilities include accounts payable, environmental, and legal liabilities.

The Coast Guard was able to make financial statement assertions and present auditable balances in actuarial pension liabilities, demonstrating limited progress toward remediation of the control and reporting

## FINANCIAL MANAGEMENT SCORECARD

	<p>deficiencies that existed in this process in FY 2008. Among the conditions that remained throughout FY 2009 is that the Coast Guard has not implemented effective policies, procedures, and controls to ensure the completeness and accuracy of medical cost data and post-employment travel claims provided to, and used by, the actuary for the calculation of the medical and post-employment benefit liabilities.</p>	
Civilian	<b>Moderate Progress</b>	
	<p>During FY 2009, the civilian components demonstrated moderate progress overall in remediating internal control weaknesses related to actuarial and other liabilities. Significant internal control weaknesses which the independent auditors identified at FLETC, ICE, and S&amp;T in FY 2008, and which contributed to a material weakness overall for the department, were fully remediated in FY 2009. However internal control deficiencies continue to exist at FEMA and new weaknesses were identified at TSA during FY 2009. These conditions at FEMA and TSA, together with the material weakness conditions at the Coast Guard, resulted in a material weakness for the department overall, in FY 2009.</p> <p>FEMA is recognized as the primary grant-making component of DHS, and the FY 2009 independent auditor's report noted that FEMA does not have sufficient policies and procedures in place to fully comply with the <i>Single Audit Act Amendments of 1996</i> and OMB Circular No. A-133, <i>Audits of States, Local Governments, and Non-profit Organizations</i>. TSA has numerous types of accounts payable and accrued liabilities that affect the balance sheet, including Other Transactions Agreements (OTA). One of the conditions at TSA that contributed to the department's material weakness is that TSA has not developed policies and procedures to accurately estimate OTA accrued liability at year-end.</p>	
<p><b>Budgetary Accounting:</b> Budgetary accounts are a category of general ledger accounts where transactions related to the receipt, obligation, and disbursement of appropriations and other authorities to obligate and spend agency resources are recorded.</p>		
Military	<b>Limited Progress</b>	
	<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 2008 remained throughout FY 2009. For example, the FY 2008 Independent Auditors' Report noted that the policies, procedures, and internal controls over the</p>	

## FINANCIAL MANAGEMENT SCORECARD

	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 weakness continues to exist in FY 2009, and remediation of these conditions is not planned for the Coast Guard until after FY 2009.	
<b>Civilian</b>	<b>Modest Progress</b>	
	<p>During FY 2008, internal control weaknesses at CBP and FEMA contributed to a departmental material weakness in this area; the material weakness continued to exist throughout FY 2009.</p> <p>For FY 2009, the department made modest progress in correcting the deficiencies that were reported in FY 2008. Although CBP implemented policies and procedures related to deobligation of funds when contracts have expired or been completed, management has not been effective in adhering to these policies or monitoring compliance. CBP has not made substantial progress in correcting the deficiencies that were reported in FY 2008. Additionally, although FEMA improved its processes and internal control over the mission assignment obligation and monitoring process, some control deficiencies remain.</p>	

## INFRASTRUCTURE PROTECTION

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

In our FY 2009 report, *Efforts to Identify Critical Infrastructure Assets and Systems*, OIG-09-86, we reported that the National Protection and Programs Directorate (NPPD) is in the process of acquiring the Infrastructure Information Collection System, a replacement for the

National Asset Database.<sup>34</sup> It is envisioned that the Infrastructure Information Collection System will greatly reduce critical infrastructure risk management gaps by providing dynamic information collection systems that include a range of relevant sources. In addition, the Infrastructure Information Collection System will allow relevant critical infrastructure partners from federal, state, local, and private entities to access various tools that house infrastructure data. Until this system is fully implemented, decision making regarding CI/KR will continue to be a significant challenge.

Concerning DHS's efforts to protect the cyber infrastructure, we reported in August 2009 that the National Cyber Security Division (NCSA) had implemented its Control Systems Security Program (CSSP) to coordinate the cybersecurity efforts for control systems between the public and private sectors.<sup>35</sup> We reported that while NCSA has made progress in implementing a cybersecurity program for control systems, opportunities exist for improvements to its CSSP. For example, NCSA needs to encourage more information sharing of critical infrastructures needs, threats, and vulnerabilities between the public and private sectors. NCSA also needs to increase the number of cybersecurity vulnerability assessments performed in order to reduce the overall risk to current operational control systems.

Also in FY 2009, we will evaluate how DHS coordinates its infrastructure protection efforts with other federal agencies, state and local governments and industry partners by reviewing the protection of petroleum and natural gas infrastructure within the energy sector. This review will determine (1) to what extent Protective Security Advisors (PSAs) are aligned to support the NPPD's primary national preparedness mission and the department's overall critical infrastructure protection strategy; (2) whether adequate guidance and resources have been provided to support the PSA program's growth; (3) the methods that PSAs use in coordinating efforts to identify, prioritize, and assess critical infrastructure and key resources within the Petroleum and Natural Gas subsectors; (4) how petroleum and natural gas stakeholders use the work that is done by PSAs; and (5) the metrics that the PSA Program uses to assess its own performance.

## **BORDER SECURITY**

A principle DHS challenge is to secure the borders against all threats, including minimizing illegal entry of persons into the U.S. To achieve this goal the U.S. Customs and Border Protection (CBP's) security mission is to obtain operational control of the border. In this effort, CBP is implementing the Secure Border Initiative (SBI), a comprehensive multi-year approach to controlling the border including immigration enforcement within the United States.

SBI-net is the program component of the SBI which will integrate personnel, infrastructure, technologies, and rapid response capability into a comprehensive border protection system. SBI-net is intended to give our frontline officers the best possible environment to effectively

---

<sup>34</sup>DHS-OIG, *Efforts to Identify Critical Infrastructure Assets and Systems*, (OIG-09-86, June 2009).

<sup>35</sup> DHS-OIG, *Challenges Remain in DHS' Efforts to Secure Control Systems* (OIG-09-95, August 2009).

detect, identify and classify, respond to, and resolve situations that compromise border security.

CBP faces challenges implementing SBI and SBInet. CBP has not established adequate controls and effective oversight of contract workers responsible for providing SBI program support services. Although CBP has recently taken steps to improve SBI program management by hiring knowledgeable and experienced program managers, it continues to rely heavily on contract personnel, who comprise more than 50% of the SBI workforce. Also, CBP has not provided an adequate number of contracting officer's technical representatives to oversee support services contractors' performance resulting in contractors performing functions that should be performed by government workers.<sup>36</sup> We are evaluating controls to ensure effective oversight of the prime contractor's performance in meeting small business goals and SBInet program costs and schedule.

Border Patrol assessments could better document and define operational requirements for tactical infrastructure to ensure that border fence construction is linked to resource decisions and mission performance goals. Furthermore, CPB did not complete 56 (77%) of the 73 rapid response Border Patrol facilities projects it planned to complete in 2008 to support its border security mission. These projects include new facilities, modifications to existing facilities, and temporary solutions to accommodate new agents and shifting agent deployments. CBP also has not replaced Border Patrol vehicles at the required 20% annual rate and does not have a centralized information system to monitor vehicle availability. CBP initiated several actions to improve its design guide, develop a new project management tracking system, and update the space planning and cost estimation tool. In addition, CBP has taken actions to improve its overall management of vehicles.<sup>37</sup>

In addition, DHS needs to focus on improving the policies, processes, and procedures that govern the management and care of its detainee population. Prior reviews of ICE's detention and removal operations identified deficiencies in the oversight of immigration detention facilities. ICE has made efforts to strengthen the oversight of ICE detention assets by establishing a Detention Facilities Inspection Group (DFIG). The DFIG provides ICE with an independent inspection arm dedicated to oversight of ICE's Detention and Removal Operations (DRO) program. Additionally, ICE has contracted with private companies to provide on-site compliance verification of the Performance-Based National Detention Standards at all ICE detention facilities. However, we recently reported that ICE could further improve documenting the transfer of immigrant detainees and ensuring they received timely medical screenings and physical examinations, required by detention standards.<sup>38</sup> Additionally, ICE

---

<sup>36</sup> DHS-OIG, *Better Oversight Needed of Support Services Contractors in Secure Border Initiative Programs*, (OIG-09-80, June 2009); and DHS-OIG, *Progress in Addressing Secure Border Initiative Operational Requirements and Constructing the Southwest Border Fence*, (OIG-09-56, April 2009).

<sup>37</sup> DHS-OIG, *CBP's Construction of Border Patrol Facilities and Acquisition of Vehicles*, (OIG-09-91, July 2009).

<sup>38</sup> DHS-OIG, *Immigration and Customs Enforcement's Tracking and Transfers of Detainees*, (OIG-09-41, March 2009).

needs to determine whether its approach to managing the detention facility bed space is cost-effective.<sup>39</sup>

## TRANSPORTATION SECURITY

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

### Checkpoint and Checked Baggage

The *Aviation and Transportation Security Act*<sup>40</sup> requires TSA to prescribe requirements for screening or inspecting all passengers, goods, and property before entry into the sterile areas of an airport. Our undercover audit of checked baggage screener performance revealed that improvements are needed in the screening process to ensure that dangerous prohibited items that enter the checked baggage system are not cleared for loading onto a passenger aircraft.<sup>41</sup> We recently issued a classified report on our unannounced, covert testing using fake law enforcement badges and credentials at selected domestic airports.<sup>42</sup> We tested equipment and techniques at the screening checkpoint to assess how well TSA is addressing the related challenges. We released a report on TSA's controls over screener uniforms, badges, and identification cards<sup>43</sup> and determined that TSA does not have adequate controls in place to manage and account for airport security identification display area badges, TSA uniforms, and TSA identification cards. Unauthorized individuals' access to those items increases an airport's level of risk to a wide variety of terrorist and criminal acts.

---

<sup>39</sup> DHS-OIG, *Immigration and Customs Enforcement Detention Bedspace Management*, (OIG-09-52, April 2009).

<sup>40</sup> Public Law 107-71, November 19, 2001.

<sup>41</sup> DHS-OIG, *Audit of the Effectiveness of the Checked Baggage Screening System and Procedures Used to Identify and Resolve Threats*, (OIG-09-42, March 2009).

<sup>42</sup> DHS-OIG, *Penetration Testing of Law Enforcement Credentials Used to Bypass Screening*, (OIG-09-99, September 2009 – Classified "Secret".)

<sup>43</sup> DHS-OIG, *TSA's Controls over SIDA Badges, Uniforms, and Identification Cards*, (OIG-08-92, September 2008).

## Passenger Air Cargo Security

Approximately 7,500 tons of cargo are carried on passenger planes each day. Federal regulations (49 CFR) require that, with limited exceptions, passenger aircraft may only transport cargo originating from a shipper that is verifiably “known” either to the aircraft operator or to the indirect air carrier that has tendered the cargo to the aircraft operator. Our audit determined that the criteria and guidance for evaluating a known shipper are unclear and subject to interpretation, increasing the risk that shippers may be improperly classified as known.<sup>44</sup> TSA’s inspection and testing activities do not provide adequate assurance that regulated entities are complying with the program’s requirements. Our report contained six recommendations to strengthen the controls and oversight of the program, including providing better criteria and guidance and improving inspection and testing activities. TSA generally concurred with all six recommendations in our report.

## Rail and Mass Transit

Recent events on the rail and transit systems in Washington DC, including a derailment, fire, and crash, have raised questions regarding the mass transit agencies’ contingency plans and the ability to handle these basic issues, as well as major emergencies. The *Aviation and Transportation Security Act* assigned TSA the responsibility to secure all modes of transportation in the United States. During emergencies, transit agencies rely on well-designed and regularly practiced drills and exercises to respond and recover rapidly. TSA created the Surface Transportation Security Inspection Program in 2005 to provide oversight and assistance to surface transportation modes. Surface Transportation Security Inspectors act as assessors, advisors, and liaisons, primarily in the mass transit and freight rail modes.

In our FY 2009 report, *Effectiveness of TSA’s Surface Transportation Security Inspectors*, OIG-09-24, we reported that TSA is improving security in the mass transit and freight rail modes through the inspection program. Inspectors help bus and passenger rail stakeholders identify security gaps through Baseline Assessment for Security Enhancement reviews. They increase TSA’s domain awareness by producing station profiles and by acting as liaisons between the Transportation Security Operations Center and transportation systems. They also participate in Visible Intermodal Prevention and Response exercises, which provide an unannounced, high-visibility presence in a mass transit or passenger rail environment. TSA faces important challenges in improving the effectiveness of the Surface Transportation Security Inspectors.

As TSA expands its presence in non-aviation modes, it must look critically at how it is deploying resources. TSA must continue to assess how planned exercises can better use the inspectors and their activities.

---

<sup>44</sup> DHS-OIG, *TSA’s Known Shipper Program*, (OIG-09-35, March 2009).

## TRADE OPERATIONS AND SECURITY

CBP is primarily responsible for trade operations and security, with the support of the Coast Guard and ICE. In 2008, approximately 11 million oceangoing cargo containers arrived at the nation's seaports. 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.

To manage the threat and ensure the security of this large volume of maritime cargo, CBP employs a multilayered approach including analyzing screening shipment information, and using targeting systems to identify the highest risk cargo on which to focus its limited resources. An effective inspection process includes the screening of shipping information, nonintrusive inspections, and physical examinations. The Automated Targeting System (ATS), which uses a complex model of weighted rules, assists CBP officers in screening shipping information and selecting shipments for inspection.

While targeting high risk shipments continues to be challenge for CBP, it can improve its operations by updating its guidance relating to the physical examinations of high-risk cargo containers that may contain biological, chemical, nuclear, and radiological threats. In addition, CBP should conduct a risk assessment to determine which pathways, including maritime cargo, pose the highest risk of biological and chemical weapons entering the Nation.<sup>45</sup>

We also reviewed DHS' planning, management oversight, and implementation of security measures to protect against small vessel threats.<sup>46</sup> Overall, the department has made progress in the area of small vessel security, but more remains to be done to provide effective guidance and programs to address small vessel threats and the potential impact these threats could have on our nation's ports and trade operations. DHS should address all the desirable characteristics and elements of an effective national strategy in its Small Vessel Security Strategy and implementation plan and it should evaluate the effectiveness of programs intended to support small vessel security before including them as part of a solution to improve security against the small vessel threats.

Additionally, one of the most significant challenges that remain is CBP's efforts to implement Section 1701 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, which requires DHS to screen all cargo headed for the United States that is loaded on or after July 1, 2012. To meet the goal of 100% screening, CBP has implemented the Secure Freight Initiative to screen 100% of cargo from select ports. However, there are

---

<sup>45</sup> DHS-OIG, *CBP's Ability to Detect Biological and Chemical Threats in Maritime Cargo Containers*, (OIG-10-01, October 2009).

<sup>46</sup> DHS-OIG, *DHS' Strategy and Plans to Counter Small Vessel Threats Need Improvement*, (OIG-09-100, September 2009).

numerous challenges that remain before this can be implemented for all cargo inbound to the U.S. Chief among these challenges is obtaining international agreements for 100% scanning and working with the international community to resolve issues concerning resources, costs, timing, and enforcement considerations.

## **Appendix A**

### **Report Distribution**

---

#### **Department of Homeland Security**

Secretary  
Deputy Secretary  
Chief of Staff for Operations  
Deputy Chief of Staff for Policy  
Deputy Chiefs of Staff  
General Counsel  
Executive Secretariat  
Director, GAO/OIG Liaison Office  
Assistant Secretary for Office of Policy  
Assistant Secretary for Office of Public Affairs  
Assistant Secretary for Legislative Affairs  
Under Secretary Management  
Chief Financial Officer  
Chief Information Officer  
Chief Security Officer  
Chief Privacy Officer

#### **Office of Management and Budget**

Chief, Homeland Security Branch  
DHS OIG Budget Examiner

#### **Congress**

Congressional Oversight and Appropriations Committees, as appropriate



#### ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at [www.dhs.gov/oig](http://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](mailto: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.