STATEMENT OF ANNE L. RICHARDS

ASSISTANT INSPECTOR GENERAL FOR AUDIT

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT, THE FEDERAL WORKFORCE, AND THE DISTRICT OF COLUMBIA

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

U.S. SENATE

DECEMBER 15, 2009

Good morning, Mr. Chairman and Members of the Subcommittee. I am Anne L. Richards, Assistant Inspector General for Audit for the Department of Homeland Security (DHS). Thank you for the opportunity to discuss the major management challenges facing DHS.

Since its inception in 2003, DHS has worked to accomplish the largest reorganization of the federal government in more than half a century. This task, creating the third largest Cabinet agency with the missions of protecting the country against another terrorist attack, responding to threats and hazards, ensuring safe and secure borders, welcoming lawful immigrants and visitors, and promoting the free flow of commerce, has presented many challenges to its managers and employees. While DHS has made progress, it still has much to do to establish a cohesive, efficient, and effective organization.

The major management challenges that we identify facing DHS represent risk areas that we use in setting our priorities for audits, inspections, and evaluations of DHS programs and operations. These challenges are included in the department's *Annual Financial Report*, which was issued on November 16, 2009. As required by the Reports Consolidation Act of 2000, we update our assessment of management challenges annually. Our latest major management challenges report covers a broad range of issues, including both program and administrative challenges. In total, we identified nine categories of challenges including Acquisition Management, Information Technology Management, Emergency Management, Grants Management, Financial Management, Infrastructure Protection, Border Security, Transportation Security, and Trade Operations and Security. A copy of that report is provided for the record. I believe the department recognizes the significance of these challenges and understands that addressing them will take a sustained and focused effort.

Today, I would like to highlight four specific management challenges facing the department:

- Acquisition management,
- Information technology management,
- Grants management, and
- Financial management.

These areas are the backbone of the department and provide the structure and information to support the accomplishment of DHS' mission. Some aspects of these challenges were inherited by the department from their legacy agencies. However, the complexity and urgency of DHS' mission have exacerbated the challenge in many areas.

These management challenges significantly affect the department's ability to carry out its operational programs and provide the services necessary to protect the homeland. The department's senior officials are well aware of these issues and are making progress in resolving them. Our oversight in these areas is intended to facilitate solutions. For example, our audits in the area of acquisition management have identified past trends and future risk areas. Also, during the past year, we issued a series of audits assessing the department's corrective action plans related to financial management improvements. We

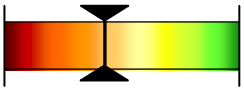
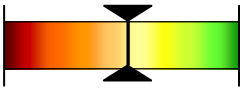
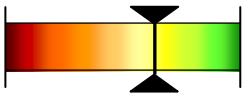
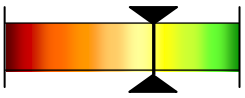
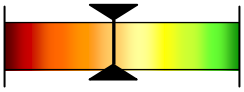
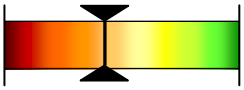
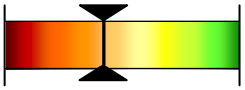
will continue our intense oversight of these management areas to ensure that solutions and corrective measures are identified and acted upon.

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. We based our scorecard ratings on a four-tiered scale ranging from limited to substantial progress[1]:

- **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.

Our overall scorecard ratings for acquisition management, information technology management, grants management, and financial management are presented in Figure 1.

Figure 1.

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

[1] Financial Management Scorecard uses different criteria to assess limited to substantial progress, and is discussed in the Financial Management section of this statement.

ACQUISITION MANAGEMENT

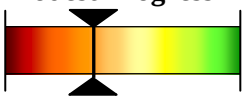
DHS relies on goods and services contractors to help fulfill many of its critical mission areas. As such, effective acquisition management is vital to achieving DHS' overall mission. Acquisition management is much more than simply awarding a contract. It requires a sound management infrastructure to 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	

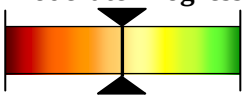
authority over all contracting through its contracting officer warrant program and Federal Acquisition Certification - Contracting program. According to the department, the heads of contracting activities and contracting officers function independently of component influence as their authority flows 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),[2] 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,[3] 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 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,[4] DHS provided guidance on award fees[5] 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

[2] GAO-09-29, *Department of Homeland Security*: *Billions Invested in Major Programs Lack Appropriate Oversight*, November 2008.
[3] DHS-OIG, *FEMA's Implementation of Best Practices in the Acquisition Process*, (OIG-09-31, February 2009).
[4] GAO-09-630, *Federal Contracting: Guidance on Award Fees Has Led to Better Practices but is Not Consistently Applied*, May 2009.
[5] 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.

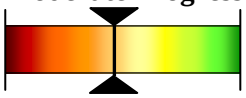
ACQUISITION MANAGEMENT SCORECARD

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.[6]

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[7] 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.[8]

In its response to our November 2008 management challenges report, DHS highlighted headquarters-level initiatives for building and retaining its acquisition workforce[9]. 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.

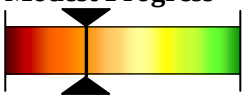
---

[6] 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).

[7] GAO-09-620T, Coast Guard: Update on Deepwater Program Management, Cost, and Acquisition Workforce, April 2009.

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

[9] *Department of Homeland Security FY 2008 Annual Financial Report.*

ACQUISITION MANAGEMENT SCORECARD	
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).[10] 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.

Security of IT Infrastructure

During our FY 2008 *Federal Information Security Management Act*[11] (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

[10] DHS-OIG, *DHS Contracts Awarded Through Other Than Full and Open Competition during Fiscal Year 2007*, (OIG-09-94, August 2009).
[11] Title III of the E-Government Act of 2002, Public Law 107-347.

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[12] 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.[13] 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, 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.[14] Specifically, we reported that DHS is experiencing delays in

[12] DHS-OIG, *Better Monitoring and Enhanced Technical Controls Are Needed to Effectively Manage LAN-A*, (OIG-09-55, April 2009).
[13] DHS-OIG, *DHS' Progress In Disaster Recovery Planning for Information Systems* (OIG-09-60, April 2009).
[14] DHS-OIG, *Improved Management and Stronger Leadership are Essential to Complete the OneNet Implementation* (OIG-09-98, September 2009).

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[15] 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[16] 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[17] 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. This office strengthened TSA's culture of privacy through coordination with managers of programs and systems that contain personally identifiable information to meet reporting requirements, performing Privacy Impact Assessments, preparing public

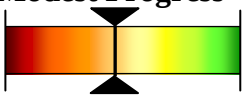
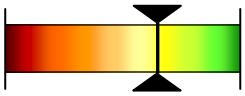
[15] DHS-OIG, *U.S. Citizenship and Immigration Services' Progress in Modernizing Information Technology* (OIG-09-90, July 2009).
[16] DHS-OIG, *Logistics Information Systems Need to be Strengthened at the Federal Emergency Management Agency*, (OIG-08-60, May 2008).
[17] DHS-OIG, *Transportation Security Administration Privacy Stewardship* (OIG-09-97, August 2009).

notifications of systems of records, and enforcing privacy rules of conduct. The office also established processes for reviewing and reporting privacy incidents, issuing public notices, addressing complaints and redress for individuals, and implementing and monitoring privacy training for employees.

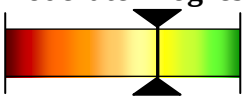
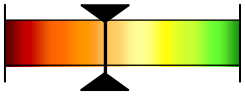
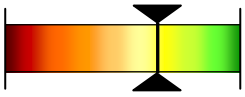
IT Management Scorecard

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

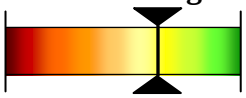
Based on the consolidated result of the six IT management capability areas, DHS has made "**moderate**" progress in IT Management overall.

IT MANAGEMENT SCORECARD	
IT Budget Oversight: ensures visibility into IT spending and alignment with the strategic IT direction.	**Modest Progress** 
The DHS CIO has made improvements in managing department-wide IT budgets in accordance with the *Clinger-Cohen Act*[18] and the department's mission and policy guidance. The DHS 2009-2013 IT Strategic Plan emphases the importance of Component IT spending approval by either the Component-level CIO or the DHS CIO. However, gaining a department-wide view of IT spending was difficult due to some Component CIOs not having sufficient budget control and insight. For example, our 2009 report[19] on U.S. Citizenship and Immigration Services (USCIS) found that it was difficult for the USCIS CIO to perform IT budgeting because business units had direct fee revenue or appropriated funds and have not complied with IT budgetary control processes. Due to the limited benefits realized, IT Budget Oversight has made "modest" progress.	
IT Strategic Planning: helps align the IT organization to support mission and business priorities.	**Moderate Progress** 
An effective IT strategic plan establishes an approach to align resources and provides a basis for articulating how the IT organization will develop and deliver capabilities to support mission and business priorities. In January 2009, the department finalized its IT	

[18] *Clinger-Cohen Act of 1996*, Public Law 104-106, Division E, Subtitle C, February 10, 1996.
[19] DHS-OIG, *U.S. Citizenship and Immigration Services' Progress in Modernizing Information Technology*, (OIG-09-90, July 2009).

IT MANAGEMENT SCORECARD	
Strategic Plan, which aligns IT goals with overall DHS strategic goals. The plan also identifies technology strengths, weaknesses, opportunities, and threats. Due to the finalization and communication of the DHS IT Strategic Plan and plans to align IT with the department's goals, this area has made "moderate" progress.	
Enterprise Architecture: functions as a blueprint to guide IT investments for the organization.	**Moderate Progress** 
The *Clinger-Cohen Act* requires that CIOs develop and implement an integrated IT architecture for the agency to avoid the risk that systems will be duplicative, not well integrated, and limited in optimizing mission performance. DHS has shown continued support of its enterprise architecture program, and has requested over $100 million of funding for fiscal year 2010. In addition, the DHS IT Strategic Plan identifies a performance measure for the percentage of IT investments reviewed and approved through the Enterprise Architecture Board. This should further promote and enforce alignment of IT investments across the department. The department has shown "moderate" progress in implementing its enterprise architecture.	
Portfolio Management: improves leadership's ability to understand interrelationships between IT investments and department priorities and goals.	**Modest Progress** 
The DHS OCIO has made "Modest" progress in establishing the department's portfolio management capabilities as instructed by OMB Circular A-130.[20] The DHS portfolio management program aims to group related IT investments into defined capability areas to support strategic goals and missions. Portfolio management improves leadership's visibility into relationships among IT assets and department mission and goals across organizational boundaries. The DHS IT Strategic Plan identifies a goal to effectively manage IT capabilities and implement cross-departmental IT portfolios that enhance mission and business performance. Although progress is being made, the department has not identified fully opportunities to standardize, consolidate, and optimize the IT infrastructure. Based on the limited benefits realized, the department has shown "modest" progress in implementing department-wide portfolio management.	
Capital Planning and Investment Control: improves the allocation of resources to benefit the strategic needs of the department.	**Moderate Progress** 

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

IT MANAGEMENT SCORECARD	
The *Clinger-Cohen Act* requires that departments and agencies create a capital planning and investment control (CPIC) process to manage the risk and maximize the value of IT acquisitions. The CPIC process is intended to improve the allocation of resources to benefit the strategic needs of the department. As part of the CPIC process, agencies are required to submit business plans for IT investments to OMB demonstrating adequate planning. To address this requirement, DHS' IT Strategic Plan communicated the importance of following the IT investment guidance provided by DHS management directive 0007.1.[21] This directive supports and expands on the Act's requirement for technology, budget, financial, and program management decisions. The department has made "moderate" progress with respect to allocation of resources to benefit its strategic needs.	
IT Security: ensures protection that is commensurate with the harm that would result from unauthorized access to information.	**Moderate Progress** 
DHS IT security is rated at "moderate," for progress made during the last 3 years in compliance with FISMA. OMB Circular A-130 requires agencies to provide protection that is commensurate with the risk and magnitude of the harm that would result from unauthorized access to information and systems assets or their loss, misuse**,** or modification. Regarding intelligence systems, information security procedures have been documented and controls have been implemented, providing an effective level of systems security.	

GRANTS MANAGEMENT

FEMA provides disaster assistance to communities through the Public Assistance Grant Program, the Hazard Mitigation Grant Program, and the Fire Management Assistance Grant Program. Under each of these grant programs, the affected State is the grantee, and the State disburses funds to eligible subgrantees. FEMA also awards grants to state and local governments; territories; tribal governments; and private, public, profit, and nonprofit organizations to enhance preparedness, protection, response, recovery, and mitigation capabilities throughout the Nation. However, improvements are needed in FEMA's grants management and oversight infrastructure to ensure effective monitoring of grantees.

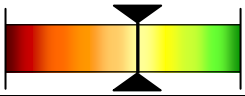
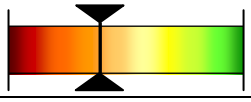
[21] DHS Management Directive 0007.1: *Information Technology Integration and Management* March 2007.

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 the most vulnerable areas and assets 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.

Grants Management

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

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

GRANTS MANAGEMENT SCORECARD	
Disaster Grants Management	**Moderate Progress** 
In FY 2008, we issued 25 financial assistance (subgrant) audit reports, identifying more than $23 million in questioned costs. As of August 2009, we had issued 41 subgrant audit reports in FY 2009, with more than $80 million in questioned costs. While FEMA does not directly manage subgrants, it is incumbent on FEMA to make certain that States, as grantees, understand the rules and regulations that govern disaster grants and ensure that subgrantees adhere to these. We plan to issue a report in early FY 2010 that presents some of the most common problems that lead to questioned costs, including inconsistent interpretation of policies by FEMA personnel and, in the case of fire assistance, problems with unsupported charges billed to subgrantees by other federal agencies that provided services.	
Non - Disaster Grants Management	**Modest Progress** 
Monitoring and documenting the effectiveness of DHS' multitude of grant programs continue to pose significant challenges 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	

GRANTS MANAGEMENT SCORECARD

disasters.

Improvements are needed in FEMA's grants management and oversight infrastructure to ensure effective monitoring of grantees. Specifically, FEMA does not consistently and comprehensively execute its two major oversight activities, financial and program monitoring. This occurs, in part, because FEMA does not have sufficient grants management staff. FEMA has not conducted the analyses and developed the plan of action required by Public Law 109-295 Title VI, the *Post Katrina Emergency Management Reform Act of 2006* as part of its strategic human capital plan. In addition, financial and programmatic monitoring policies, procedures, and plans are not comprehensive.

FEMA has formed an Intra-Agency Grants Program Task Force that has developed a FEMA Grants Strategy to drive future enhancements in grants policies, procedures, systems, and processes. The task force has identified projects including the development of comprehensive grant management monitoring policies and procedures for the FEMA directorates with program management and oversight responsibilities.

Many states, as grantees, 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 2009, we issued audit reports on homeland security grants management by Illinois and California. We are currently reviewing Massachusetts, Maryland, Missouri, South Carolina, West Virginia, and the District of Columbia. These entities generally did an efficient and effective job of administering the grant funds; however, the most prevalent areas needing improvement concerned performance measurement, subgrantee monitoring, financial documentation and reporting, and control of expenditure reimbursement requests.

FINANCIAL MANAGEMENT

DHS continued to improve financial management in FY 2009, but challenges remain. Beginning in FY 2009, our independent auditors performed an integrated financial statement and internal control over financial reporting audit limited to the DHS consolidated balance sheet and statement of custodial activity. As in previous years, our independent auditors were unable to provide an opinion on those statements because the department could not provide sufficient evidence to support its financial statements or represent that financial statement balances were correct. Additionally, the independent auditors were unable to perform procedures necessary to form an opinion on DHS' internal control over financial reporting of the balance sheet and statement of custodial activity due to the pervasiveness of the department's material weaknesses.

Although the department has continued to remediate material weaknesses and has reduced the number of conditions contributing to the disclaimer of opinion on the financial statements, all six material weakness conditions were repeated in FY 2009. Table 1 below presents a summary of the internal control findings, by component, for the Independent Auditor's Report on DHS' fiscal year 2009 Financial Statements. Table 2 provides FY 2008 information and is being included for comparative purposes. We have reported six material weaknesses and two significant deficiencies at the Department level in FY 2009, shown in Table 1.

TABLE 1 - SUMMARIZED DHS FY 2009 INTERNAL CONTROL FINDINGS

Comment / Financial Statement Area		DHS Consol.	CG	CBP	USCIS	FEMA	FLETC	ICE	NPPD	S&T	TSA
			Military	Civilian							
Material Weaknesses:			Exhibit I	Exhibit II							
A	Financial Management and Reporting	MW									
B	IT Controls and System Functionality	MW									
C	Fund Balance with Treasury	MW									
D	PP&E and OM&S	MW									
E	Actuarial and Other Liabilities	MW									
F	Budgetary Accounting	MW									
Significant Deficiencies:			Exhibit III								
G	Other Entity-Level Controls	SD									
H	Custodial Revenue and Drawback	SD									

TABLE 2 - SUMMARIZED DHS FY 2008 INTERNAL CONTROL FINDINGS

Comment / Financial Statement Area		DHS Consol.	CG	CBP	USCIS	FEMA	FLETC	ICE	NPPD	S&T	TSA
			Military	Civilian							
Material Weaknesses:			Exhibit I	Exhibit II							
A	Financial Reporting	MW									
B	IT General and App. Controls	MW									
C	Fund Balance with Treasury	MW									
D	Capital Assets and Supplies	MW									
E	Actuarial and Other Liabilities	MW									
F	Budgetary Accounting	MW									
Significant Deficiencies:			Exhibit III								
G	Entity-Level Controls	SD									
H	Custodial Revenue and Drawback	SD									
I	Deferred Revenue	SD									

	Control deficiency findings are more severe
	Control deficiency findings are less severe
MW	Material weakness at the Department level exists when all findings are aggregated
SD	Significant deficiency at the Department level exists when all findings are aggregated

Furthermore, the increase in audit scope related to auditing internal control over financial reporting resulted in our independent auditor identifying significant departmental challenges that have a pervasive impact on the effectiveness of internal controls over consolidated financial reporting. Specifically:

- The department lacks a sufficient number of accounting and financial management personnel with core technical competencies to ensure that its financial statements are presented accurately and in compliance with generally accepted accounting principals;

- DHS' accounting and financial reporting infrastructure, including policies, procedures, processes, and internal controls, have not received investments in proportion to the department's rapid growth in new programs and operations, and changes in mission since the department's inception;

- Field and operational personnel do not always share responsibilities for, or are not held accountable for, matters that affect financial management, including adhering to accounting policies and procedures and performing key internal control functions in support of financial reporting; \

- The department's financial Information Technology (IT) system infrastructure is aging and has limited functionality, which is hindering the Department's ability to implement efficient corrective actions and produce reliable financial statements that can be audited.

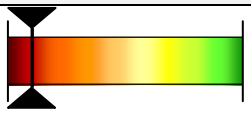
IT controls and systems functionality conditions at FEMA and ICE deteriorated in FY 2009. The remaining significant component level challenges preventing the department from obtaining an opinion on its consolidated balance sheet and statement of custodial activity are primarily at the Coast Guard and TSA. In both FY 2009 and FY 2008, Coast Guard was unable to assert to any of its account balances; and TSA was unable to fully support the accuracy and completeness of the property, plant, and equipment (PP&E) account balance. However, the Coast Guard has made limited progress implementing the *Financial Strategy for Transformation and Audit Readiness* (FSTAR) in FY 2009. As a result, the auditors have been able to perform limited audit procedures over PP&E and actuarial liabilities. Additionally, the FSTAR calls for substantially more progress after FY 2010, especially in areas necessary to assert to the completeness, existence, and accuracy of PP&E, actuarial liabilities, and fund balance with Treasury balances.

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 2008. The scorecard is divided into two categories: (1) Military – Coast Guard and (2) Civilian – all other DHS components. The scorecard lists the six material weaknesses identified during the independent audit of the FY 2008 DHS consolidated balance sheet and statement of

custodial activity. These weaknesses continued to exist throughout FY 2009 and were again noted in 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.[22] To determine the status, we compared the material weaknesses reported by the independent auditor in FY 2008 with those identified in FY 2009.[23] 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.

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

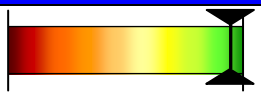
FINANCIAL MANAGEMENT SCORECARD		
Financial Reporting and Management: Financial reporting is the process of presenting financial data about an agency's financial position, the agency's operating performance, and its flow of funds for an accounting period. Financial management is the planning, directing, monitoring, organizing, and controlling of financial resources, including program analysis and evaluation, budget formulation, execution, accounting, reporting, internal controls, financial systems, grant oversight, bank cards, travel policy, appropriation-related Congressional issues and reporting, working capital funds, and other related functions.		
Military	**Limited Progress**	
	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 FY 2008 the Coast Guard revised its FSTAR; however, most of the actions outlined in the FSTAR were scheduled to occur after FY 2008. 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	

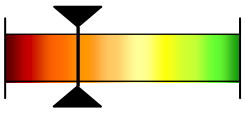
[22] DHS-OIG, *Independent Auditors' Report on DHS' FY 2008 Financial Statements*, (OIG-09-09, November 2008).
[23] DHS-OIG, *Independent Auditors' Report on DHS' FY 2009 Financial Statements and Internal Control Over Financial Reporting*, (OIG-10-11, November 2009).

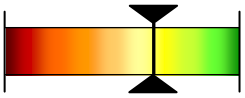
FINANCIAL MANAGEMENT SCORECARD		
	department's total liabilities. However, most corrective actions outlined in the FSTAR are scheduled to occur after FY 2009, and consequently many of the financial reporting weaknesses reported in prior years remained as of the end of FY 2009. Among the conditions at 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.	
Civilian	**Limited Progress**	
	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. 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. 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.	
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	**Limited Progress**	

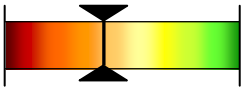
FINANCIAL MANAGEMENT SCORECARD		
	During 2008, the independent auditors identified numerous IT general control deficiencies, of which nearly all were repeat findings from prior years. The most significant IT deficiencies that could affect the reliability of the financials statements related to the development, 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. 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. 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.	
Civilian	**Limited Progress**	
	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. 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	

FINANCIAL MANAGEMENT SCORECARD		
	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.		
Military	**Limited Progress**	
	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 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.	

FINANCIAL MANAGEMENT SCORECARD		
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.	
Property, Plant, and Equipment (PP&E) and Operating Materials and Supplies (OM&S): DHS capital assets and supplies consist of items such as property, plant, and equipment, operating materials; and supplies, including boats and vessels at the Coast Guard, passenger and baggage screening equipment at TSA, and stockpiles of inventory to be used for disaster relief at FEMA.		
Military	**Limited Progress**	
	The Coast Guard maintains approximately 52 percent of the department's property, plant, and equipment (PP&E), including a large fleet of boats and vessels. In FY 2008, internal control weaknesses related to PP&E at Coast Guard contributed to a material weaknesses in this area for the department. For FY 2009, the Coast Guard has demonstrated limited progress overall in correcting internal control weaknesses related to PP&E identified in the independent auditor's report in FY 2008. During FY 2009, the Coast Guard continued implementation of its remediation plan (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 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&E balance necessary to prepare the year-end balance sheet. The auditors also identified weaknesses related to operating materials and supplies (OM&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 implemented policies, procedures, and internal controls to support financial assertions related to OM&S and related balances for FY 2009.	

FINANCIAL MANAGEMENT SCORECARD		
Civilian	**Modest Progress**	
	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 that 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	**Limited Progress**	
	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 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	

FINANCIAL MANAGEMENT SCORECARD		
	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.	
Civilian	**Moderate Progress**	
	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&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. 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 S*ingle Audit Act Amendments of 1996* and OMB Circular No. A-133, *Audits of States, Local Governments, and Non-profit Organizations.* 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.	
Budgetary Accounting: Budgetary accounts are a category of general ledger accounts where transactions related to the receipt, obligation, and disbursement of appropriations and other authorities to obligate and spend agency resources are recorded.		
Military	**Limited Progress**	
	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 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	

FINANCIAL MANAGEMENT SCORECARD		
	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.	
Civilian	**Modest Progress**	
	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. 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.	

I have highlighted four specific management challenges facing the department—financial management, information technology management, acquisition management, and grants management—that are the backbone of the department and provide the structure and information to support the accomplishment of DHS' mission. While some aspects of these challenges were inherited by the department from their legacy agencies, the complexity and urgency of DHS' mission has exacerbated the challenge in many areas.

While the department's senior officials are well aware of these problems and are making progress in resolving these issues, we must continue to keep the department focused on these challenges. Our continued oversight in these areas is intended to facilitate solutions in order to significantly improve the department's ability to carry out its operational programs.

Mr. Chairman, this concludes my prepared statement. I will be pleased to answer any questions you or the Members may have.