STATEMENT OF RICHARD L. SKINNER

INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

SUBCOMMITTEE ON HOMELAND SECURITY

COMMITTEE ON APPROPRIATIONS

U.S. HOUSE OF REPRESENTATIVES

February 13, 2008

Good morning, Mr. Chairman and Members of the Subcommittee. I am Richard L. Skinner, Inspector General 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 Statement Report (AFR), which was issued on November 15, 2007. 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:

- Catastrophic Disaster Response and Recovery,
- Acquisition Management,
- Grants Management,
- Financial Management,
- Information Technology 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:

- Financial Management,
- Information Technology Management,
- Acquisition Management, and
- Grants Management.

Also, I would like to address briefly certain critical programs challenges that need special attention during the upcoming year. These are:

- Border Security and the SBI Program,
- Coast Guard's Deepwater Acquisition Program,
- Cargo on Passenger Planes and the Known Shipper Program,
- CIS' Backlog of Immigrant Applications, and
- FEMA Preparedness.

Financial management, information technology management, acquisition management, and grants management, 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 our 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, in our *Semiannual Report to Congress*, October 1, 2006 – March 31, 2007, we included a scorecard identifying the progress made in selected acquisition functions and activities within DHS. 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.

FINANCIAL MANAGEMENT

Financial management has been a major challenge for DHS since its creation in 2003. In 2007, DHS was again unable to obtain an opinion on its financial statements, and numerous material internal control weaknesses continued to be reported. KPMG, LLP, under contract with the Office of Inspector General (OIG), has consistently issued a disclaimer of opinion on DHS' financial statements. There has been continued improvement at Customs and Border Protection (CBP) and significant improvement at Immigration and Customs Enforcement (ICE). However, the majority of the department's material weaknesses in internal control are attributable to conditions existing at the U.S. Coast Guard (Coast Guard), which has contributed to all of the department's material weaknesses in both FY 2007 and FY 2006.

Table 1 below presents a summary of the internal control findings, by component, for the Independent Auditors' Report on DHS' fiscal year 2007 Financial Statements. In all, there were seven material weaknesses at the department level in 2007, down from ten reported in 2006. While the DHS civilian components have made substantial progress in correcting control deficiencies, the reduction in material weaknesses at the department level in 2007 is due to a consolidation of findings into fewer, but broader categories for reporting purposes.

Table 1. SUMMARIZED DHS FY 2007 INTERNAL CONTROL FINDINGS

	Material Weaknesses	Coast Guard	DHS HQ	CBP	FEMA	ICE	US - Visit	TSA	FLETC
		Exhibit I	Exhibit II						
A	Financial Management & ELC	MW			MW				
B	Financial Reporting	MW	MW		MW			SD	
C	Financial Systems Security	MW	SD	SD	MW	SD		MW	SD
D	Fund Balance With Treasury	MW							
E	Capital Assets and Supplies	MW			MW		SD	SD	
F	Actuarial and Other Liabilities	MW			MW			SD	
G	Budgetary Accounting	MW			MW			MW	
	Significant Deficiencies		Exhibit III						
H	Custodial Revenue and Drawback			SD					

SD Significant Deficiency (SDs in Exhibit II contribute to department-level material weakness)

MW Material Weakness (individually, or when combined with other findings, result in department-level material weakness)

Some of the conditions contributing to the Coast Guard's material weaknesses were identified in the Department of Transportation's OIG audit of the Coast Guard Financial statement for the year ending September 30, 1994. Although, in FY 2007, the Coast Guard implemented the Financial Strategy for Transformation and Audit Readiness (FSTAR) as the corrective action plan to remediate the material weaknesses, the plan did not contain detailed milestones showing how the Coast Guard would get from the current to the desired state. Additionally, the FSTAR submission for the FY 2008 remediation does not contain detailed milestones showing how the Coast Guard will be able to remediate targeted weaknesses in FY 2008. Also, the targeted remediation milestone is December 31, 2008. As a result, the Coast Guard is not projected to remediate any material weaknesses during the FY 2008 DHS financial statement audit. FSTAR is currently under a performance audit, which should be completed during the second quarter of FY 2008.

Additionally, in FY 2007, conditions at the Federal Emergency Management Agency (FEMA) deteriorated with FEMA now contributing to six material weaknesses instead of two material weaknesses as in FY 2006. FEMA has submitted Management Action Plans (MAP) with milestones to remediate the material weaknesses in 2008. These plans are currently under a performance audit, which should be completed during the second quarter of FY 2008.

DHS' material internal control weaknesses ranged from financial management reporting at the department level to financial management and controls surrounding the recording of individual account balances within DHS components. These control weaknesses, due to their materiality, are impediments to obtaining a clean opinion and providing positive assurance over internal controls at the department level. Achieving these departmental goals is highly dependent on internal control improvements at the Coast Guard, FEMA, the Transportation Security Administration (TSA), and the Office of the Chief Financial Officer (CFO).

To move forward, DHS must develop a comprehensive, financial management strategy that addresses organizational resources and capabilities, inconsistent and flawed business processes, and unreliable financial systems. In 2006, DHS took the initial step in this process by preparing comprehensive corrective action plans to address known internal control weaknesses. The corrective action plans from each component were incorporated into a single management strategy document identified as the Internal Control Over Financial Reporting (ICOFR) playbook. The DHS CFO, with the support of executive leadership and the involvement of component financial management, has aggressively pursued corrective actions throughout FY 2007. As a result, with the exception of FEMA, the corrective action plans for DHS' nonmilitary components have started to show results in improving financial reporting during FY 2007, although overall, the department still has much work remaining.

During fiscal year 2008, we anticipate progress in addressing some internal control deficiencies. We will perform a series of performance audits later this year, which are intended to assess the extent of progress and the status of planned corrective actions. These audits will be completed and available in the second quarter of FY 2008. Further, conditions reported as material weaknesses in internal controls in previous independent auditor reports will be updated and reported in the FY 2008 Consolidated Financial Statement Audit Report on or before November 15, 2008.

In addition, FEMA issued approximately 2,700 mission assignments totaling about $7.2 billion to federal agencies to help with the response to Hurricane Katrina. FEMA historically has had significant problems issuing, tracking, monitoring, and closing mission assignments. FEMA guidance on mission assignments is often vague, and agencies' accounting practices vary significantly, causing problems with reconciling agencies' records to FEMA records. FEMA has developed a number of new, predefined mission assignments to streamline some of the initial recurring response activities. In addition, FEMA's Disaster Finance Center is working to find a consensus among other federal agencies on appropriate supporting documentation for billings. We are conducting a review of mission assignments to DHS agencies and other Inspectors General are reviewing mission assignments to their respective agencies.

INFORMATION TECHNOLOGY MANAGEMENT

One of DHS' biggest challenges remains integrating the information technology (IT) systems, networks, and capabilities of the various legacy agencies to form a single infrastructure for effective communications and information exchange. There are multiple aspects to achieving such an IT infrastructure, as outlined below.

Security of Information Technology Infrastructure

The security of the IT infrastructure is a major management challenge. As we reported in September 2007, based on its annual *Federal Information Security Management Act* evaluation, and excluding its intelligence systems, DHS continues to improve and strengthen its security program. DHS implemented a performance plan to measure each

component's progress toward full compliance with its information security program. The performance plan tracks key elements indicative of a strong, functioning security program. Despite this oversight, components again are not executing fully the department's policies, procedures, and practices. Issues remain with component system certification and accreditation, Plans of Action and Milestones, and system baseline configurations. Other information security program areas where weaknesses exist include security configuration management, incident detection and analysis, and security training. Management oversight of the component's implementation of the department's policies and procedures needs to be improved to ensure the quality of the certification and accreditation process, and that all information security weaknesses are tracked and remediated.

In addition to our Federal Information Security Management Act (FISMA) evaluations, during the past year we conducted information security audits of DHS laptop computers, and performed technical security evaluations at Ronald Reagan Washington National Airport and Dulles International Airport. We assessed protective measures for personally identifiable information, and evaluated physical and system security at Plum Island. We also reviewed major programs and applications, such as DHS' implementation of Homeland Security Presidential Directive (HSPD-12) and the Automated Targeting System.

Based on the results of these audits, as well as our FISMA evaluation, and despite continued improvements in DHS' information security program, we determined that DHS organizational components are not executing all of the department's policies, procedures, and practices. For example:

- All operational systems have not been adequately certified and accredited;

- All components' information security weaknesses are not included in a Plan of Action and Milestones; and

- Standard configurations have not been fully implemented.

Further, while DHS has issued substantial guidance designed to create and maintain secure systems, there exist areas where agency-wide information security procedures require strengthening:

- Certification and accreditation;
- Vulnerability testing and remediation;
- Contingency plan testing;
- Incident detection, analysis, and reporting;
- Security configurations; and
- Specialized security training.
-

To address these issues, the CIO must identify ways to improve the review process and increase the accountability of DHS component organizations.

Additionally, DHS is required to protect its intelligence systems. We reported that DHS should grant the Office of Intelligence and Analysis (OI&A) the comprehensive authority to support the management, operation, and security of the department's Sensitive Compartmented Information systems. This authority will strengthen OI&A's oversight of component compliance with FISMA requirements for the data and the information systems that support its intelligence operations and assets. Later this year we will report on the results of our audit of the department's security program and practices affecting IT intelligence operations and assets.

Department-wide IT Infrastructure

Creating an adequate disaster recovery capability for DHS' information systems is a major concern. DHS' IT infrastructure remains a collection of legacy networks, systems, and data centers. Several elements of this IT infrastructure do not have the ability to relocate to an alternate site that can be used if their primary facility suffers an extended outage or becomes inaccessible. This inability to restore the functionality of DHS' critical IT systems following a service disruption or disaster could negatively affect accomplishment of a number of essential DHS missions, including passenger screening, grants processing, and controlling the flow of goods across U.S. borders.

DHS has focused on this issue by establishing the National Center for Critical Information Processing and Storage (NCCIPS). The NCCIPS is to provide hosting of departmental applications, network connectivity, and critical data storage under the direction of DHS' Chief Information Officer (CIO). In FY 2007, DHS awarded a contract for a second data center to supplement NCCIPS. DHS listed the second data center as a large, redundant, secure, scalable capability that will provide DHS with sufficient backup, disaster recovery, and continuity of operations in an emergency. The NCCIPS and the second data center are to have "active-active" processing capability to ensure each mission-critical system has a complete disaster recovery capability. DHS plans to close 16 existing data centers by moving their processing to the new active-active processing data centers.

Due to a lack of identified funding for migration of systems, DHS has been hindered in its efforts to establish the NCCIPS as an alternate processing facility. Specifically, DHS has stated that migration of systems to NCCIPS will be based on availability of funding, not on criticality of the system. Ensuring that the initial funds provided are spent effectively and will enable DHS to achieve the desired disaster recovery capability in a timely fashion will involve significant resources, oversight, and senior management attention.

Similarly, upgrading the DHS data communications infrastructure and consolidating the various organizations that provide data communications support are major undertakings for DHS. Coordinating these related communications upgrade efforts would require significant resources and oversight. Further, DHS will need to demonstrate how it will achieve the envisioned cost savings. Ensuring that DHS data communications activities remain effective and secure during the upgrade and transition also is a major concern.

DHS Component IT Management

Although improvements have been made, IT management at the subcomponent level remains a major challenge, as demonstrated by our audits and subsequent reports on the IT programs and initiatives of selected DHS directorates and organizations. We continued to identify problems with outdated or stove-piped systems, at times supporting inefficient business processes. Planning to modernize IT was unfocused, often with inadequate requirements identification, analysis, and testing to support acquisition and deployment of the systems and other technologies needed to improve operations. We also found consideration of privacy matters to be lacking for some IT programs.

For example, in November 2006, we reported as part of a followup review that U.S. Citizenship and Immigration Services (USCIS) had made some progress by placing priority on business transformation. USCIS was taking steps to centralize authority for IT personnel, initiating business process reengineering activities, and upgrading desktops and servers at key field locations.[1] However, we found that USCIS would benefit from improvements in centralizing IT operations and refining IT management practices. To be successful, USCIS also must continue to ensure that its transformation strategy, as defined, is clearly executed. We concluded that until USCIS addresses these issues, the bureau would not be in a position to manage existing workloads or handle the potentially dramatic increase in immigration benefits processing workloads that could result from proposed immigration reform legislation.

Similarly, our December 2006 followup assessment of FEMA's efforts to upgrade its principal disaster management system showed that although the agency has made short-term progress in addressing problems in each of these areas, more remains to be done to address long-term planning and systems integration needs. These improvements primarily included increasing the National Emergency Management Information System's (NEMIS) capacity and online access and registration. In addition, FEMA and its program offices specifically addressed our previous report's recommendations by documenting training resources, developing a plan to implement its enterprise architecture, gathering requirements for new business tools, and improving configuration management.

Despite these positive steps, FEMA had not documented or communicated a strategic direction to guide long-term IT investment and system development efforts. FEMA also had not performed crosscutting requirements gathering to determine business needs, which would allow its Information Technology Services Division (ITSD) personnel to analyze alternatives to continued development of the complex, custom NEMIS system. FEMA has challenges to accomplishing these tasks, including personnel needs, time limitations, and funding constraints. Therefore, constrained by limited resources, FEMA focused its efforts on preparing for the 2007 hurricane season and made little progress in addressing long-term needs, such as updating strategic plans, defining cross-cutting requirements, and evaluating systems alternatives.

[1] DHS-OIG, *U.S. Citizenship and Immigration Services' Progress in Modernizing Information Technology*, OIG-07-11, November 2006.

Our reviews of major IT programs and initiatives of various components' management indicate similar problems. For example, in June 2007, we reported that a key Science and Technology (S&T) data mining program, Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE) was at risk, due to a number of factors.[2] Specifically, S&T program managers did not develop a formal business case for the research and development project, in part because they were unaware of requirements to do so. In addition, program managers did not address privacy impacts before implementing three pilot initiatives to support ADVISE. Further, due to inadequate data access and system usability, OI&A analysts did not use the ADVISE pilot. Finally, because S&T did not effectively communicate and coordinate with DHS leadership about the benefits of ADVISE, departmental components have been unwilling to adopt ADVISE to support their intelligence analysis operations. DHS discontinued the three ADVISE pilots due to privacy concerns and ultimately announced the termination of the ADVISE program in September 2007.

In July 2007, we reported that the National Bio-Surveillance Integration System (NBIS) program was falling short of its objectives.[3] Specifically, DHS did not provide consistent leadership and staff support to ensure successful execution of the NBIS program. For various reasons, NBIS ownership shifted among department organizations numerous times, with corresponding fluctuations in the program approach, priority, and accomplishments. NBIS also struggled since its inception to secure the staff needed to manage program activities effectively. As a result of the repeated transitions and staffing shortfalls, planning documents needed to guide IT development were not finalized. Program management did not effectively communicate and coordinate with stakeholders to secure the data, personnel, and information sharing agreements needed to support system development. Additionally, program management did not provide the contractor with adequate guidance, requirements input, or data sources to deliver a fully functional system. As such, the contractor may not fulfill NBIS capability and schedule requirements, which potentially could result in cost increases to the program.

Information Sharing

The *Homeland Security Act of 2002*[4] makes coordination of homeland security communication with state and local government authorities, the private sector, and the public a key DHS responsibility. Due to time pressures, DHS did not complete a number of the steps essential to effective planning and implementation of the Homeland Security Information Network (HSIN)—the sensitive but unclassified system it instituted to help carry out this mission.

As we reported in June 2006, DHS did not clearly define HSIN's relationship to existing collaboration systems and also did not obtain and address requirements from all HSIN

[2] DHS-OIG, *ADVISE Could Support Intelligence Analysis More Effectively*, OIG-07-56, June 2007.
[3] DHS-OIG, *Better Management Needed for the National Bio-Surveillance Integration System Program*, OIG-07-61, July 2007.
[4] P.L. 107-296.

user communities in developing the system.[5] Further, DHS did not provide adequate user guidance, including clear information sharing processes, training, and reference materials. Without establishing a baseline and developing specific performance measures, DHS had no effective way to track or assess information sharing using HSIN. As of June 2007, DHS' Office of Operations Coordination had taken steps to address our report's recommendations. Specifically, to remedy communication, coordination, and system guidance shortfalls, program management has created an HSIN Joint Program Office to develop training initiatives. Also, a Stakeholder Relationship Management team was tasked to focus on engagement of stakeholders and communicating the mission and vision of HSIN. In addition, the Homeland Security Information Network Work Group was engaged in aligning business processes, coordinating requirements, and creating cross-functional governances for HSIN. Lastly, the HSIN Program Manager was working to ensure that performance metrics were established, instituted, and used to determine system and information sharing effectiveness.

On a broader scale, DHS is challenged with incorporating data mining into its overall strategy for sharing information to help detect and prevent terrorism. Data mining aids agents, investigators, and analysts in the discovery of patterns and relationships from vast quantities of data. *The Homeland Security Act* authorizes DHS to use data mining and other tools to access, receive, and analyze information. Our August 2006 report on DHS data mining activities identified various stove-piped activities that use limited data mining features.[6] For example, CBP performs matching in order to target high-risk cargo. The U.S. Secret Service automates the evaluation of counterfeit documents. TSA collects tactical information on suspicious activities. ICE detects and links anomalies indicative of criminal activity to discover relationships. However, without department-wide planning, coordination, and direction, the potential for integrating advanced data mining functionality and capabilities to address homeland security issues remains untapped.

ACQUISITION MANAGEMENT

Balancing Urgency and Good Business Practices

With DHS annually spending about 39 % of its budget through contracts, effective acquisition management is fundamental to DHS' ability to accomplish its missions. Due to our current homeland security vulnerabilities, DHS tends to focus its acquisition strategies on the urgency of meeting mission needs, rather than balancing urgency with good business practices. Excessive attention to urgency without good business practices leaves DHS and the taxpayers vulnerable to spending millions of dollars on unproductive homeland security investments. Acquisitions must provide good value, because funds spent ineffectively are not available for other, more beneficial uses.

[5] DHS-OIG, *Homeland Security Information Network Could Support Information Sharing More Effectively*, OIG-06-38, June 2006.
[6] DHS-OIG, *Survey of DHS Data Mining Activities,* OIG-06-56, August 2006.

We have conducted audits and reviews of individual DHS contracts, such as the Coast Guard's Deepwater program and CBP Secure Border Initiative Network. Common themes and risks emerged from these audits, primarily the dominant influence of expediency, poorly defined requirements, and inadequate oversight that contributed to ineffective or inefficient results and increased costs. Numerous opportunities exist for DHS to make better use of good business practices, such as well-defined operational requirements and effective monitoring tools, that would have preserved the government's ability to hold poorly performing contractors accountable.

Suspension and debarment are the most serious methods available to hold government contractors accountable for failed performance and to protect the government's interests in future procurements. To ensure the government has the option of using these methods, along with other tools to hold contractors accountable, the government must lay the groundwork from the very beginning of the acquisition process. That is, contracts must specify precisely expected outcomes and performance measures, and the government must properly oversee contractor performance. Without these basic provisions, the government will have no basis to assert that a contractor failed to perform, and thus, no basis to pursue suspension and debarment to protect the taxpayers in future procurements.

The urgency and complexity of DHS' mission will continue to demand rapid pursuit of major acquisition programs. As DHS builds its acquisition management capabilities in the components and department-wide, the business of DHS goes on and major procurements continue to move. Acquisition is not just awarding a contract, but an entire process that begins with identifying a mission need and developing a strategy to fulfill that need through a thoughtful, balanced approach that considers cost, schedule, and performance. Urgent acquisitions need more discipline, not less, because the consequences of failure are higher. DHS needs to distinguish between truly urgent needs and less urgent needs.

Programs developed at top speed sometimes overlook key issues during program planning and development of mission requirements. Also, an over-emphasis on expedient contract awards may hinder competition, which frequently results in increased costs. Finally, expediting program schedules and contract awards limits time available for adequate procurement planning and development of technical requirements, acceptance criteria, and performance measures. This can lead to higher costs, schedule delays, and systems that do not meet mission objectives.

One procurement method DHS uses is performance-based contracting. While this method has certain advantages over traditional, specifications-based contracting, it also introduces risks that, unless properly managed, threaten achievement of cost, schedule, performance, and, ultimately, mission objectives.

Sound business practice is a performance-based acquisition strategy to address the challenges of DHS' programs. Partnering with the private sector adds fresh perspective, insight, creative energy, and innovation. It shifts the focus from traditional acquisition models, i.e., strict contract compliance, to one of collaborative, performance-oriented

teamwork with a focus on performance, improvement, and innovation. Nevertheless, using this type of approach does not come without risks. To ensure that this partnership is successful, DHS must lay the foundation to oversee and assess contractor performance, and control costs and schedules. This requires more effort and smarter processes to administer and oversee the contractors' work. Therein lies the critical importance of describing mission needs, and the yardsticks by which to measure achievement, completely and precisely. Without clear agreement between the government and the contractor about what the procurement is to achieve, the government is vulnerable to cost overruns, delays, and, in the end, not receiving a good or service that meets its needs.

Performance-based contracting may have additional risks, but with forethought and vigorous oversight, the risks can be managed. "[R]isk management is the art and science of planning, assessing, and handling future events to ensure favorable outcomes. The alternative to risk management is crisis management, a resource-intensive process…" with generally more limited options.[7] While no one has yet formulated the perfect risk management solution, risks can be controlled, avoided, assumed, or transferred. For example, programs can develop alternative designs that use lower risk approaches, competing systems that meet the same performance requirements, or extensive testing and prototyping that demonstrates performance. Risk mitigation measures usually are specific to each procurement. The nature of the goods and services procured, the delivery schedule, and dollars involved determine what mitigation is appropriate.

A balanced approach is more likely to result in obtaining the right products and services at the right times for the right prices. Little disagreement exists about the need for our Nation to protect itself immediately against the range of threats, both natural and manmade, that we face. At the same time, the urgency and complexity of the department's mission create an environment in which many programs have acquisitions with a high risk of cost overruns, mismanagement, or failure. Adopting lower risk acquisition approaches that better protect the government's interests enhance the department's ability to take action against bad actors.

An Efficient, Effective, and Accountable Acquisition Function

We published the first of what will be a series of scorecards identifying the progress made in selected acquisition functions and activities within DHS.[8] The data included in the scorecards reflect our audits and inspections reports issued through March 2007, as well as additional fieldwork conducted in February 2007 and March 2007. We used GAO's *Framework for Assessing the Acquisition Function at Federal Agencies* (September 2005) and DHS' *Acquisition Oversight Program Guidebook* (July 2005) as a baseline.

[7] Department of Defense, Defense Acquisition University, *Risk Management Guide for DoD Acquisition*, Fifth Edition (Version 2.0), June 2003.
[8] DHS Office of Inspector General, *Semiannual Report to the Congress*, October 1, 2006 – March 31, 2007, pages 59 – 78.

These references identify the following five interrelated elements essential to an efficient, effective, and accountable acquisition process:

- Organizational alignment and leadership;
- Policies and processes;
- Financial accountability;
- Acquisition workforce; and
- Knowledge management and information systems.

The Office of the Chief Procurement Officer is the DHS organization with responsibility for all department acquisition activities and services. This includes management, administration and oversight, financial assistance, and strategic and competitive sourcing. Responsibilities also include the development and publication of department-wide acquisition and financial assistance regulations, directives, policies, and procedures. Each component head shares responsibility for the acquisition function with the DHS Chief Procurement Officer. Therefore, the Chief Procurement Officer has used collaboration and cooperation with the components as the primary means of managing DHS-wide acquisition oversight. Specifically, some collaborative methods include integrating departmental components through common policies and procedures, meeting monthly with component procurement managers, and providing input on component new hires and procurement employees' performances.

Our audits and reviews during the past year continue to indicate that deficiencies persist. For example, there is still:

- Lack of strong acquisition authority in the Office of the Chief Procurement Officer and less than full partnership with other departmental functions;
- Lack of comprehensive program management policies and processes;
- Ineffective internal control over financial reporting;
- Insufficient program management staffing; and
- Unreliable information systems that are not integrated and do not provide useful reports and analysis.

DHS acquisition leaders identified some progress, but previously reported deficiencies remain largely uncorrected. Many remaining acquisition challenges fall outside the Office of the Chief Procurement Officer's control. A brief summary of each element follows.

Organizational Alignment and Leadership. DHS executive leadership has made modest progress in ensuring that the acquisition function achieves the organizational alignment needed to perform. Strong executive leadership is needed to ensure that the importance of the acquisition function is acknowledged and integrated with all other functions involved in, or affected by, procurement activities. One area of improvement is the increased communication by acquisition leadership to inform staff about the role and importance of their mission to DHS. The atmosphere for collaboration between DHS and its components on acquisition matters has improved. However, many still view the

acquisition function as a support activity, i.e., a contract processing office, rather than as a partner. Acquisition has begun to receive more resources for staffing and training.

Policies and Processes. DHS has made modest progress in developing policies and processes to ensure that components comply with regulations, policies, and processes to achieve department-wide goals. In 2005, DHS issued a management directive and guidebook that established policies and procedures for oversight of DHS acquisitions, with the common goal of delivering mission results while maintaining compliance with applicable laws, regulations, policies, and procedures. An acquisition manual and additional acquisition regulations for DHS have also been developed. According to GAO and our recent reports and interviews with DHS officials, the need still remains for a comprehensive DHS approach to program management standards.

Financial Accountability. DHS has made limited progress in ensuring financial oversight and accountability within the acquisition function. DHS financial information is generally unreliable, and financial systems do not have the internal controls and integration that acquisition personnel require. Also, the acquisition and finance offices have not successfully partnered on acquisition planning and strategic decision-making. DHS has numerous and persistent issues with inadequate internal controls and data verification. Improper payments have been made, and there are few checks on data once it is recorded in the system. This problem is exacerbated by the use of multiple, nonintegrated information technology systems across the department. Without a reliable data system, it has been very difficult for the financial office to make an impact in the broader acquisition process.

Acquisition Workforce. The capabilities of DHS' acquisition workforce will determine, to a great extent, whether major acquisitions fulfill DHS' urgent and complex mission needs. Contracting officers, program managers, and Contracting Officer Technical Representatives (COTRs) make critical decisions on a nearly daily basis that increase or decrease an acquisition's likelihood of success. DHS has made modest progress in building a skilled acquisition workforce. However, until a fully trained acquisition workforce is developed, it will be difficult to achieve further progress needed for an efficient, effective, and accountable acquisition function.

Both our office and the GAO have reported that the Office of the Chief Procurement Officer needs more staff and authority to carry out its oversight responsibilities. GAO recommended that DHS provide the Office of the Chief Procurement Officer sufficient resources and enforcement authority to enable effective, department-wide oversight of acquisition policies and procedures. We made a similar recommendation. An increase in the personnel budget has allowed DHS to fill many needed acquisition staff positions. Also, the number of oversight specialists in the Acquisition Oversight Division is authorized to expand to 40 during fiscal year 2008. However, the division has fewer than 10 staff on-board. Competition with other departments for acquisition personnel is intense. The Office of the Chief Procurement Office has undertaken an outreach program to involve DHS component staff to manage effectively and assist in acquisition oversight. In previous reports, our office and GAO identified the need for additional certified

program managers. The Office of the Chief Procurement Officer subsequently created a training program that likely will increase the pool of certified program managers.

Office of Personnel Management data indicates that more than 40 % of DHS' contracting officers will be eligible to retire within the next 5 years. To mitigate this circumstance, DHS plans to use additional appropriations to hire more personnel and implement an acquisition internship program that will bring in junior staff.

Knowledge Management and Information Systems. DHS has made limited progress since its creation in developing and deploying information systems to track and analyze acquisition data and improve user efficiency. Current systems are not fully integrated, contain unreliable input, and do not have internal controls to verify data. As a result, the acquisition program cannot effectively provide information to its stakeholders and does not have the tools necessary for planning or monitoring its transactions. Many DHS components still maintain their legacy contract writing systems and DHS lacks integration between contract writing and contract management systems. DHS has selected PRISM as its standard contract writing system, but the department-wide rollout is behind schedule. Integration and data accuracy problems will continue to exist until all components migrate to the same contract writing system.

U.S. Coast Guard Deepwater Acquisition

The Integrated Deepwater System Program (Deepwater) is a $24 billion, 25-year acquisition program designed to replace, modernize, and sustain the Coast Guard's aging and deteriorating fleet of ships and aircraft, providing a deepwater capable fleet for 40 years.[9] The Deepwater acquisition strategy is a nontraditional systems-of-systems approach by which private industry was asked to not only develop and propose an optimal mix of assets, infrastructure, information systems, and people-based solution designed to accomplish all of the Coast Guard's Deepwater missions, but also to provide the assets, the systems integration, integrated logistics support, and the program management. Under a more traditional acquisition strategy, the government would contract separately for each major activity or asset involved, such as cutters and aircraft, and their logistics support, communications equipment, systems integration, and program management operations.

Audits and other reviews of the Coast Guard's Deepwater Program have identified a number of management challenges and risks that raise fundamental questions about the viability of the Coast Guard's "System of System" strategy for recapitalizing and upgrading its Deepwater fleet of small boats, patrol boats, cutters, helicopters, and fixed-wing aircraft.

[9] The Deepwater area of operations is typically defined as beyond the normal operating range, approximately 50 miles from shore.

These challenges and risks include:

- A Deepwater acquisition work force that lacks the requisite training, experience, certification, and structure to acquire assets and systems of significant scope and complexity;

- A contract structure that did not easily adapt to the environment of changing missions and requirements, and major systems integration;

- The reliance on a lead systems integrator to manage day-to-day issues associated with the Deepwater Program;

- The Coast Guard's reticence to enforce contract performance requirements; and

- The Coast Guard's acceptance of contractor self-certification of technical standards in lieu of independent third-party certification.

To its credit, Coast Guard has acknowledged these problems and taken aggressive action to resolve them. Specifically, the Coast Guard has:

- Initiated action to consolidate all Coast Guard acquisition functions under one directorate;

- Reasserted its technical authority over Deepwater acquisitions;

- Increased its use of independent, third party assessments; and

- Redefined the Deepwater contract terms and conditions.

Coast Guard has also acted aggressively to improve its contract and technical oversight of the Deepwater Program by:

- Reinstituting its role as technical authority as opposed to the contractor when making decisions.

- Assuming the role of the decision-making authority as lead integrator and Integrated Product Team leader, a role Coast Guard had previously been delegated to the contractor.

- Initiating a process for reviewing engineering changes to improve control over the changes and associated costs.

- Contracting for an independent third-party review to validate proposed technical solutions for the **N**ational **S**ecurity **C**utters.

- Initiating a comprehensive independent third-party analysis of the entire Integrated Deepwater System to identify and document the most resource efficient method of satisfying an identified mission capability gap, including life cycle cost estimates and a cost-benefit analysis.

The Coast Guard and ICGS also renegotiated the 2002 Deepwater contract cost, schedule, and performance baselines of National Security Cutters 1, 2, and 3 in August 2007. The purpose of which was to address the terms and conditions that the Department and the Coast Guard considered to be unfavorable to the U.S. Government. As a result of the negotiations, the contracts for National Security Cutters #2 and #3 were changed from firm-fixed price to cost-plus-incentive fee, and there are now cost control incentives for the contractor. Additionally, the action incorporates a Navy best practice that requires the contractor to provide, on a quarterly basis, a release and notification of any conduct or action the contractor considers to be a potential change to the contract. Additionally, the Coast Guard cancelled the acquisition of the Vertical Unmanned Aerial Vehicle and the Short Range Prosecutor due to technical concerns and is working on developing cost-effective alternatives.

Overall, we believe the Coast Guard has made significant progress to improve the accountability of Integrated Coast Guard Systems and other Deepwater contractors. We will continue to exercise oversight over this very important and mission critical acquisition.

FEMA Acquisitions

In the aftermath of Hurricane Katrina, FEMA was not prepared to provide the kind of acquisition support needed for a catastrophic disaster. Specifically, FEMA lacked:

- Sufficient acquisition planning and preparation for many crucial acquisitions needed immediately after the disaster;

- Clearly communicated acquisition responsibilities among FEMA, other federal agencies, and state and local governments; and

- Sufficient numbers of acquisition personnel to manage and oversee contracts.

Pursuant to the Post-Katrina Emergency Management Reform Act of 2006 (Post-Katrina Act), FEMA has undergone significant reorganization, including in its acquisition function. Major concerns for the acquisition program included the need for:

- An integrated acquisition system;

- Comprehensive program management policies and processes;

- Appropriate staffing levels and trained personnel;

- Reliable and integrated financial and information systems; and

- Timely corrective actions in response to many OIG and GAO report recommendations.

FEMA has recognized the need to improve acquisition outcomes and has taken positive steps that include:

- Using a hurricane gap analysis tool to identify potential disaster response gaps;

- Executing prenegotiated or "readiness" contracts in advance of disasters;

- Working with DHS' Disaster Response/Recovery Internal Control Oversight Board to address response problems; and

- Increasing from 35 contracting staff when Hurricane Katrina struck to the 130 FEMA now has on-board.

However, challenges remain. FEMA needs to continue its progress in (1) hiring and training qualified acquisition staff, and (2) developing a fully integrated and sustainable acquisition management system, before it gains full control over its acquisition management program.

Outlook and OIG Oversight

DHS can protect the public interest in major acquisitions. The long-run solutions include:

- Strong program and procurement offices;
- Clearly articulated program goals;
- Defined program technical requirements, performance measures, and acceptance terms;
- Well-structured contracts; and
- Thorough cost and performance oversight.

In the near term, DHS can mitigate risks and limit government's exposure through such actions as the following:

- Writing shorter-term contracts with smaller, incremental tasks;
- Using contract vehicles that better share risk between government and vendor; and
- Ensuring that the government retains negotiating power with decision points and options.

We will continue a vigorous audit and investigation program to uncover DHS acquisition vulnerabilities and recommend swift, cost-effective improvements. Acquisition management is and will continue to be a priority for my office and an area where we

focus considerable resources. Our plan is to continue examining such crosscutting acquisition issues as workforce qualifications, competition, small and disadvantaged business utilization, and corporate compliance, in addition to individual programs, such as Deepwater and the Secure Border Initiative.

GRANTS MANAGEMENT

In conjunction with the realignment efforts being undertaken pursuant to the Post-Katrina Act, the grant programs administered by the Office of Grants and Training transferred to FEMA, effective April 1, 2007. Grants and Training grant management activities were absorbed within two new FEMA Directorates. Grants and Training's grant business and administrative management functions will be centralized in the Grant Programs Directorate, while program management functions will become a part of the National Preparedness Directorate.

Grants and Training's financial management activities, which were previously provided by Grants and Training's legacy organization at the Department of Justice, will be absorbed by FEMA's Office of the Chief Financial Officer (OCFO) during FY 2008. The OCFO will be responsible for all financial grants management functions within the new FEMA. Financial grants management encompasses all financial activities necessary to manage the grant funds, from appropriation through closeout of the grant award. As a result, FEMA directly oversees more than 80 % of all grant resources awarded by DHS. This includes not only mitigation programs, but also preparedness grants valued at nearly $4 billion in FY 2007.

Recognizing that this was a mid-year transition, the processes in place to announce Grants and Training grant guidance, receive and review applications, and announce awards remained unchanged in FY 2007. The relationship between Grants and Training grantees and Preparedness Officers in providing grant guidance and other services also remained unchanged. The Grants Management System (GMS) supports the grant management process involving the receipt of grant applications and grant processing activities.

For the short-term, FEMA will run two financial systems: (1) FEMA GMS, and (2) Grants and Training GMS. This will allow FEMA to incorporate all Grants and Training financial data, including grants data, within the new FEMA. Grants and Training GMS includes grantee payment functionality and financial status reporting capabilities. In FY 2008, Grants and Training GMS data will migrate to FEMA GMS to form a unified system.

Managing the multitude of grant programs within DHS poses a significant challenge. The grant programs of other federal agencies that assist states and local governments in improving their abilities to prepare for, respond to, and recover from acts of terrorism or natural disasters compound this challenge. The Congress continues to authorize and appropriate funding for individual grant programs within and outside of DHS for similar, if not identical, purposes. In total, DHS manages more than 80 disaster and nondisaster grant programs. For disaster response and recovery efforts, we have identified 36 federal

assistance programs that have the potential for duplicating DHS grant programs. In addition, the internal DHS reorganization has compounded these issues, as overlapping jurisdictions and systems must be reconciled. DHS must do more to coordinate and manage grants that are stove-piped for specific, but often related purposes, to ensure that they are contributing to our highest national preparedness and disaster recovery goals, rather than duplicating one another and being wasted on low-priority capabilities.

The administration has authorized more than $132 billion to support recovery efforts in the nation's Gulf Coast as a consequence of hurricanes Katrina, Wilma, and Rita. In the Gulf Coast states affected by these hurricanes, numerous federal grants from different agencies and components of DHS are going to state and local governments, private organizations, and individuals for response and recovery from these hurricanes, as well as for the next disaster or terrorist attack. We are currently reviewing disaster grant activities throughout the Gulf Coast and will continue to give special emphasis to Gulf Coast disaster response and recovery grant spending.

In FY 2008, DHS is expecting to award approximately $3.2 billion for state and local preparedness expenditures, as well as assistance to firefighters. Of this amount, $2.2 billion is requested for DHS to fund grant, training, and exercise programs under FEMA. In addition, in coordination with the state preparedness grant program, FEMA will be administering the $1 billion Public Safety Interoperable Communications grant program in partnership with the Department of Commerce.

We are reviewing individual state's management of first responder grants and the effectiveness of DHS' system for collecting data on state and local governments' risk, vulnerability, and needs assessments. Our audits have reported on the states' inability to effectively manage and monitor these funds, and demonstrate and measure improvements in domestic security. Our reports also pointed out the need for DHS to monitor the preparedness of state and local governments, grant expenditures, and grantee adherence to the financial terms and conditions of the awards.[10]

[10] DHS OIG: *The State of Georgia's Management of State Homeland Security Grants Awarded During Fiscal Years 2002 through 2004*, OIG-08-22, January 2008, *The State of Florida's Management of State Homeland Security Grants Awarded During Fiscal Years 2002 through 2004*, OIG-08-20, December 2007, *The Commonwealth of Pennsylvania's Management of State Homeland Security Grants Awarded During Fiscal Years 2002 through 2004*, OIG-08-03, October 2007, *The State of New Jersey's Management of State Homeland Security Grants Awarded During Fiscal Years 2002 through 2004*, OIG-07-58, July 2007; *Audit of State Homeland Security Grants Awarded to the American Samoa Government*, OIG-07-42, May 2007; *The State of North Carolina's Management of State Homeland Security Grants Awarded During Fiscal Years 2002 and 2003*, OIG-07-02, October 2006; *Audit of Emergency Management Performance Grant Funds Awarded to the Virgin Islands Territorial Emergency Management Agency*, DA-07-01, October 2006; *The Commonwealth of Virginia's Management of State Homeland Security Grants Awarded During Fiscal Years 2002 and 2003*, OIG-06-45, July 2006; *Audit of Grant 2004-TK-TX-003 and 2005-GH-T5-0001 Awarded to the National Domestic Preparedness Coalition of Orlando, Florida*, OIG-06-34, May 2006; and *The State of Indiana's Management of State Homeland Security Grants Awarded During Fiscal Years 2002 and 2003*, OIG-06-19, December 2005.

Given the billions of dollars appropriated annually for disaster and nondisaster grant programs, DHS needs to ensure that internal controls are in place and adhered to, and grants are sufficiently monitored to achieve successful outcomes. DHS must ensure that, to the maximum extent possible, disaster and homeland security assistance go to those states, local governments, private organizations, or individuals eligible to receive such assistance and that grantees adhere to the terms and conditions of the grant awards. DHS needs to continue refining its risk-based approach to awarding first responder grants to ensure that areas and assets that represent the greatest vulnerability to the public are as secure as possible. It must incorporate sound risk management principles and methodologies to successfully prepare for, respond to, recover from, and mitigate acts of terrorism and natural disasters.

DHS management recognizes these challenges. DHS is planning a study to provide a single grants management system for all nondisaster-related grants. In addition, a risk-based grant allocation process was completed in FY 2006. DHS risk analysis was a critical component of the process by which allocations were determined for such programs as the Homeland Security Grant Program, Transit Security Grant Program, Port Security Grant Program, and the Buffer Zone Protection Program.

Finally, Mr. Chairman, I would like to highlight briefly other critical challenges that the department needs to keep a close eye on over the next twelve months as the country prepares for a national election and transitions to a new administration.

- Border Security and the SBI Program,
- Coast Guard's Deepwater Acquisition Program,
- Security Over Cargo on Passenger Planes,
- CIS' Backlog of Immigrant Applications, and
- FEMA Preparedness.

These initiatives are in a critical stage of their development and, therefore, require unwavering management attention. Although the department is making a good faith effort to formulate and execute meaningful performance plans to address the management challenges associated with these initiatives, the ability of the department to sustain these efforts is fragile at this point in time because of the early stage they are in and the disruptions that may accompany the transition to the new administration in less than a year. It is imperative that the department formulate comprehensible performance plans with unambiguous milestones and metrics to gauge or measure progress, ensure transparency and accountability, and help guide program execution.

Border Security and the SBI Program

A principal DHS challenge is reducing America's vulnerability to terrorism by controlling the borders of the United States. To this end, DHS is implementing the Secure Border Initiative (SBI), a comprehensive multi-year activity to secure the borders and reduce illegal immigration. CBP, ICE, CIS, and the Coast Guard all have key roles in the SBI program. To ensure SBI success, it is critical that the program is thoroughly

planned. DHS also must institute an approach to coordinating the SBI functions and activities of the participating DHS components with the related efforts of other agencies as well. We are currently conducting a series of audits to evaluate whether the SBI program initiatives are being accomplished in an economical, efficient, and effective manner.

Coast Guard's Deepwater Acquisition Program

The aged and deteriorating condition of the Coast Guard's aircraft, boats, and cutters is impacting the Coast Guard's readiness to perform its missions. Recent reports of hull and mechanical failures involving the Coast Guard's largest and oldest cutters clearly demonstrate that urgent action is needed. The Deepwater Acquisition program, designed to recapitalize Coast Guard's fleet of assets, has not met cost, schedule, and performance expectations.

To help place the Deepwater Acquisition on sound footing, Congress mandated that no funds should be available for Deepwater procurements until an independent third party completed an Alternatives Analysis to identify and document the most resource-efficient method of resolving mission capability gaps. The Analysis, which to be completed by February 28, 2008, is critical in determining the number and mix of assets to be procured under the revised Deepwater Implementation Plan. Coast Guard's implementation of the revised Deepwater Implementation Plan is critical to Coast Guard's ability to effectively carry out its missions.

Security Over Cargo on Passenger Planes

H.R.1: Implementing Recommendations of the 9/11 Commission Act of 2007, requires DHS to establish a system to screen 100 percent of cargo transported on passenger aircraft by August 2010. Current TSA regulations require air carriers to screen 30 percent of cargo that has not been exempted from screening, which can be accomplished through physical examinations or non-intrusive methods, such as x-ray systems, explosives detection systems, and certified canine inspection teams. Regulations also require that cargo to be transported on passenger aircraft come from known shippers although there are exceptions where cargo from unknown shippers may be transported.

Our audits, as well as prior GAO work, have identified a number of weaknesses in TSA's multi-layered approach to oversee and ensure air carrier compliance with cargo screening requirements. For example, our review of TSA's air cargo security program found that a large percentage of cargo is entirely exempt from screening, TSA has limited resources to conduct inspections, and its inspectors rely primarily on reviewing air carrier documentation only after cargo has been transported to verify compliance with federal security regulations.

Moving to 100 percent screening of air cargo on passenger plans presents a huge challenge for TSA. TSA is currently piloting a voluntary program to permit cargo screening by certified entities at additional points along the supply chain. TSA will

continue to utilize the Known Shipper Program, which provides a systematic approach to assess risk and determine the legitimacy of shippers. Congress has asked GAO to review the agency's efforts to comply with requirements of the 9/11 Act by conducting a review of the Certified Cargo Screening Program, and has requested that we conduct a review the Known Shipper Program to determine the extent to which cargo from unknown shippers is being transported on passenger aircraft.

CIS' Backlog of Immigrant Applications

A key factor in this effort will be the progress CIS makes in modernizing its information technology systems. CIS has developed a number of plans to modernize its systems, but none of them have been implemented fully. As noted earlier in this testimony, we reported in November 2006 that until USCIS improves IT management and operations, the bureau will not be in a position to either effectively manage existing workloads or handle the potentially dramatic increase in immigration benefits processing workloads that could result from proposed immigration reform legislation.

FEMA Preparedness

We are currently reviewing and evaluating FEMA's preparedness for effective disaster response, including any catastrophic events. This review is the second in a planned series of scorecard assessments to determine the extent of progress made and the status for selected functions and activities within the Department of Homeland Security (DHS). For this scorecard review, we identified nine key program functions critical to successful preparedness efforts: Overall Planning; Coordination and Support; Interoperable Communications; Logistics; Evacuations; Housing; Disaster (Surge) Workforce; Mission Assignments; and Acquisition Management. Within each of these functions, we are assessing FEMA's progress and identified improvements needed in two to five critical action areas.

* * * * * * * * * * * *

Mr. Chairman, this concludes my prepared statement. 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.

I will be pleased to answer any questions you or the Members may have.