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 6, 2007

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 *Performance and Accountability Report*, which was issued on November 15, 2006. 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 and Contract 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.

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. In November, we issued an SBInet Risk Advisory report with recommendations for better managing the risks associated with this major procurement.

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 2006, 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.

DHS' material internal control weaknesses ranged from financial management oversight and reporting at the department level to controls surrounding the recording of individual account balances within DHS bureaus. 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 upon internal control improvements at the United States Coast Guard (USCG), Immigration and Customs Enforcement (ICE), the Transportation Security Administration (TSA), and the Office of the Chief Financial Officer.

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. An initial step in this process is to prepare well-developed and comprehensive corrective action plans to address known internal control weaknesses. During this past year, the department has taken a thoughtful approach to developing such a plan and has begun to implement corrective actions.

Concurrent with the department's efforts, we initiated a series of performance audits to assess the effectiveness of DHS' corrective action plans to address internal control weaknesses. Our objective in conducting these performance audits was to determine the thoroughness and completeness of both the overall corrective action plan process and individual component plans developed to address specific financial control weaknesses. These performance audits are intended to provide ongoing feedback to DHS as it is developing and implementing corrective action plans.

During fiscal year 2006, we anticipated progress in addressing internal control deficiencies. DHS identified four areas for improvement during the year. However, in our corrective action plan audits, we reported that a coordinated, department-wide effort to develop corrective action plans did not begin until the third quarter of 2006 and is now in the process of being finalized. At the component level, we identified well-developed corrective action plans at ICE, but significant work remains ahead for the Coast Guard. During 2006, ICE began its corrective action plan process early and our audit results showed internal control improvements during the fiscal year.

In addition, the Federal Emergency Management Agency (FEMA) issued approximately 2,700 mission assignments totaling about $8.7 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

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 remains one of DHS' biggest challenges. 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 another major management challenge. As we reported in September 2006, based upon its annual Federal Information Security Management Act evaluation, excluding its intelligence systems, DHS achieved a significant milestone toward strengthening its information security program by implementing a department-wide remediation plan to certify and accredit all operational systems by the end of fiscal year 2006. Further, some of the means to assist DHS and its components in the implementation of its information assurance program, which we identified in our fiscal year 2005 Federal Information Security Management Act report, also have been addressed, such as developing a process to maintain a comprehensive inventory.

However, additional information security audits we conducted this past year showed challenges remain in controlling and addressing a number of IT risks and vulnerabilities. These audits involved DHS networks, databases, laptops, and Radio Frequency Identification systems, as well as of major programs such as the Transportation Workers Identification Credential and United States Visitor and Immigrant Status Indicator Technology.

Specifically, DHS organizational components, through their Information Systems Security Managers, have not completely aligned their respective information security programs with DHS' overall policies, procedures, and practices. 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 Chief Information Officer must identify ways to improve the review process and increase the accountability of DHS component organizations. The department also must establish a comprehensive management authority to ensure the confidentiality, integrity, and availability of its vital intelligence information.

Department-wide IT Infrastructure

Creating an adequate capability for relocating mission-critical information systems to an alternate disaster recovery site in the event of extended service disruptions or emergencies is one concern. The department's 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. However, due to a lack of sufficient funding and an operational program to support an enterprise-wide disaster recovery solution, DHS has been hindered in its efforts to provide an alternate processing facility. 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.

Similarly, significant resources and oversight are also needed to accomplish the major undertakings of upgrading the DHS data communications infrastructure and consolidating the various organizations that provide data communications support. Currently, the department is in the process of eliminating redundant firewalls, replacing hardware encryption devices, and combining operations centers—activities that are essential to supporting the efficient, effective, and secure exchange of mission-critical information both within DHS and with outside stakeholders.

DHS Component IT Management

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. Our November 2006 followup assessment reports that the United States Citizenship and Immigration Services (USCIS) has made some progress by placing priority on business transformation, taking steps to centralize authority for IT personnel, initiating business process reengineering activities, and upgrading desktops and servers at key field locations. However, USCIS remains entrenched in a cycle of

continual planning, with limited progress toward achieving its long-term transformation goals. Until USCIS addresses this issue, the bureau will 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 shows that the agency has made progress in meeting short-term systems needs; however, more remains to be done to address long-term planning and systems integration.

Our reviews of major IT programs and initiatives of the various components also indicate program management problems. For example, in September 2005, we reported that FEMA could benefit from improvements to its 6-year, $1.5 billion program to digitize the maps used to identify flood zones and determine insurance requirements. Although FEMA is making progress in the flood map modernization program, FEMA can better ensure program success by:

- Reviewing and revising its mapping plan,
- Enhancing program guidance,
- Increasing contractor oversight,
- Improving coordination with stakeholders,
- Clearly defining requirements and contractor expectations, and
- Maintaining standard methodologies for mapping system development.

Similarly, in August 2006, we reported on improvements USCG could make in its efforts to design and implement command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems as part of its estimated $24 billion Integrated Deepwater System (Deepwater) program. Although the USCG has made progress in the program, problems with contract oversight, requirements management, systems certification and accreditation, and IT testing place the Deepwater IT acquisition and C4ISR operations at risk. Insufficient C4ISR funding has restricted accomplishing the "system-of-systems" objectives that are fundamental to ensuring interoperability of Deepwater assets, such as ships and aircraft. Meeting the training and IT support needs of Deepwater C4ISR users also is key.

Information Sharing

The Homeland Security Act of 2002 makes coordination of homeland security communication with state and local government authorities, the private sector, and the public a key DHS responsibility. However, 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 such, effective sharing of the counter-terrorist and emergency management information critical to ensuring homeland security remains an ongoing challenge for the department. Resources, legislative constraints, privacy, and cultural challenges—often beyond the control of HSIN program management—pose obstacles to HSIN's success.

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 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. For example, Customs and Border Protection performs matching to target high-risk cargo. The United States 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.

Hurricane Katrina also highlighted the need for data sharing among federal agencies following a catastrophic disaster. We see a need for data sharing in three areas:

- Real-time data exchange among agencies would help verify eligibility of applicants for disaster assistance and simplify the application process for victims.
- Direct access to FEMA data by law enforcement agencies would help identify and track convicted sex offenders and suspected felons, and help locate missing children.
- Computer data matching would help to prevent duplicative payments and identify fraud.

FEMA is moving in the right directions on these issues. For example, FEMA has granted direct access to its data to the Hurricane Katrina Fraud Task Force for the purpose of investigating fraud. However, progress is slow and much remains to be done. FEMA and the federal community are not ready to meet the data sharing demands of the next catastrophic disaster.

Another example of vital information sharing is the National Asset Database. The National Infrastructure Protection Plan envisions a comprehensive, national inventory of assets, known as the National Asset Database, to help DHS coordinate the effort to protect the nation's critical infrastructure and key resources. DHS is responsible for integrating efforts to protect the chemical industry; commercial facilities; dams; emergency services; commercial nuclear reactors, materials, and waste; information technology; telecommunications; postal and shipping; transportation systems; and government facilities. A maturing National Asset Database is essential to developing a comprehensive picture of the nation's critical infrastructure and key resources. Management and risk-based resource allocation decisions depend on having this comprehensive picture. As we reported in fiscal year 2006, DHS is improving the development and quality of the National Asset Database. We will continue to monitor and review how DHS uses the National Asset Database to support its risk management framework, how it coordinates infrastructure protection with other sectors, and how its

pursuit of basic vulnerability assessment standards can help develop overarching departmental priorities.

ACQUISITION AND CONTRACT MANAGEMENT

Acquisition management is not just awarding a contract, but fulfilling a mission need through a thoughtful, balanced approach that considers cost, schedule, and performance. The urgency and complexity of DHS' mission will continue to demand rapid pursuit of major investment programs. In 2006, DHS spent about 40% of its budget through contracts.

DHS must have an infrastructure in place that enables it to oversee effectively the complex and large dollar procurements critically important to achieving the DHS mission. While DHS continues to build its acquisition management capabilities in the component agencies and on the department-wide level, the business of DHS goes on and major procurements continue to move. We identified significant risks and vulnerabilities that might threaten the integrity of DHS' acquisition management program. In general, DHS needs to improve its major acquisitions planning, operational requirements definition, and implementation oversight.

The prerequisite for effective acquisitions, that is, obtaining the right, cost-effective systems and equipment to accomplish DHS' missions, is program management. Complex and high-dollar contracts require multiple program managers, often with varying types of expertise. Several DHS procurements have encountered problems because contract technical and performance requirements were not well defined. DHS needs:

- More certified program managers;
- Comprehensive department-wide standards for program management;
- A strengthened investment review board process to provide greater independent analysis and review;
- Better defined technical requirements; and
- More balance among schedule, cost, and performance when expediting contracts.

The Office of the Chief Procurement Officer recently established a program management advisory board, established standards for certifying program managers, and promoted program management training opportunities. The Office of the Chief Procurement Officer is assisting program offices with acquisition planning, including templates and one-on-one assistance.

In their transition into DHS, seven agencies retained their procurement functions, including USCG, FEMA, and TSA. The expertise and capability of the seven procurement offices mirrored the expertise and capability they had before creation of DHS, with staff size that ranged from 21 to 346 procurement personnel. DHS established an eighth acquisition office, the Office of Procurement Operations, under the direct

supervision of the Chief Procurement Officer, to service the other DHS components and manage department-wide procurements. Many DHS procurement offices reported that their lack of staffing prevents proper procurement planning and severely limits their ability to monitor contractor performance and conduct effective contract administration. The fiscal year 2007 DHS Appropriations Act provides over 400 additional contract specialist positions to alleviate part of the shortfall. Moreover, DHS is planning a contracting fellows program with up to 100 entry-level positions to begin in fiscal year 2008.

In addition to awarding contracts, the Office of the Chief Procurement Officer helps DHS components adhere to standards of conduct and federal acquisition regulations in awarding and administering contracts. This oversight role involves developing department-wide policies and procedures, and enforcing those policies and procedures.

Both our office and the Government Accountability Office have reported that the Office of the Chief Procurement Officer needs more staff and authority to carry out its general oversight responsibilities. The Government Accountability Office recommended that DHS provide 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. The DHS, in response to our December 2006 report, *Major Management Challenges Facing the Department of Homeland Security*, said that it disseminated the Acquisition Professional Management Directive to identify and certify appropriately trained and experienced program managers, contracting officer's technical representatives, and authorized buying agents. It also has certified 348 program managers since 2004, and continues to focus on qualifications and placement.

During fiscal year 2006, the Under Secretary for Management established policies for acquisition oversight and directed each of the eight heads of contracting activities to measure and manage their acquisition organizations. Also, the number of oversight specialists in the Acquisition Oversight Division is authorized to expand to nine during fiscal year 2007. 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.

Common Themes in Our Audits of DHS Contracts

In prior years, we conducted audits and reviews of individual DHS contracts, such as TSA's screener recruiting and TSA's information technology services. More recently, we have completed audits relating to the SBInet program, the Coast Guard's Deepwater program, and FEMA contracting. 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.

The department continues to pursue high-risk, complex, system-of-systems acquisitions programs, such as SBInet and Deepwater. A performance-based acquisition strategy to address the challenges of these programs is, in our opinion, a good one. 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, into 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, the department 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.

Customs and Border Protection SBInet Program

On November 2, 2005, DHS announced a multiyear strategy to secure America's borders and reduce illegal immigration, called the Secure Border Initiative (SBI). A critical element of the SBI initiative is the acquisition of technology, infrastructure, and personnel to gain operational control of the nation's border – SBInet. The SBInet procurement presents a considerable acquisition risk because of its size and scope. We see risks and vulnerabilities similar to those identified in previous OIG audits and reviews.

Customs and Border Protection awarded a multiple-year systems integration contract in September 2006 to begin the SBInet multibillion dollar initiative. We have monitored the initiation of the SBInet program and provided a risk advisory with recommendations to address observed weaknesses in the program. The department was fully responsive during our SBInet review, agreed to our recommendations, and is planning and pursuing corrective actions. However, the SBInet procurement continues to present a considerable acquisition risk because of its size and scope.

Our main concern about SBInet is that DHS is embarking on this multibillion dollar acquisition project without having laid the foundation to oversee and assess contractor performance and effectively control cost and schedule. DHS has not properly defined, validated, and stabilized operational requirements and needs to do so quickly to avoid rework of the contractor's systems engineering and the attendant waste of resources and delay in implementation. Moreover, until the operational and contract requirements are firm, effective performance management, and cost and schedule control, are precluded. As acknowledged in our report, the department took actions to mitigate risk during the course of our review and is planning further actions to establish an effective performance management system for SBInet.

We also reported that the department does not have the capacity needed to effectively plan, oversee, and execute the SBInet program; administer its contracts; and control costs and schedule. The department's acquisition management function lacks the appropriate work force, business processes, and management controls for planning and executing a major acquisition program such as SBInet. Without a preexisting professional acquisition

workforce, Customs and Border Protection has had to create staffing plans, locate workspace, and establish business processes, while simultaneously initiating one of the largest acquisition programs in the department. DHS needs to move quickly to establish the organizational capacity to properly oversee, manage, and execute the program.

Coast Guard's Deepwater Program

USCG has also encountered a number of challenges in executing its Deepwater Acquisition program despite the expenditure of more than $3 billion over 4 years. This is particularly true within the Deepwater surface and air domains. Most recently, we identified management deficiencies and inadequate technical oversight related to the acquisition of the National Security Cutter. In this case, the Coast Guard did not exercise sufficient oversight authority of the contract with Integrated Coast Guard Systems to address design deficiencies. Consequently, the National Security Cutter acquisition is expected to cost more than originally planned and the cutters may be subject to operational limitations that affect the ability of the Coast Guard to execute its Deepwater mission.

Similar issues were previously identified related to the 110-foot patrol boat conversion project. This project was curtailed at eight cutters due to design, construction, performance, and cost concerns. In December, the Coast Guard decided to take the eight converted cutters out of service due to structural design deficiencies. In response to these challenges, USCG accelerated plans to design, construct, and deploy the composite Fast Response Cutter by more than 10 years as a replacement for the 110-foot patrol boat. However, an independent analysis has confirmed that the Fast Response Cutter design is outside patrol boat design parameters, i.e., too heavy, too overpowered, and not streamlined enough to reduce resistance. These concerns led to the USCG's April 2006 decision to suspend work on the Fast Response Cutter until these issues could be resolved or an alternative commercial off-the-shelf design identified.

In the Deepwater air domain, the HH-65C helicopter and unmanned aerial vehicle acquisitions have encountered schedule delays and cost increases. These Deepwater design, construction, performance, scheduling, and cost issues are expected to continue to present significant challenges to USCG's Deepwater Program in the future.

The Coast Guard recognizes these challenges and is taking aggressive actions to strengthen program management and oversight—such as technical authority designation; use of independent, third party assessments; consolidation of acquisition activities under one directorate; and redefinition of the contract terms and conditions, including award fee criteria. Furthermore, and most importantly, the Coast Guard is increasing its staffing for the Deepwater program, and reinvigorating its acquisition training and certification processes to ensure that staff have the requisite skills and education needed to manage the program. These steps should go a long way in improving the management and oversight of the Deepwater program as it moves forward.

FEMA Procurements

We have also focused substantial work on FEMA contracting and have identified numerous problems. FEMA is not well prepared to provide the kind of acquisition support needed for a catastrophic disaster. FEMA's overall response efforts suffer from:

- Inadequate acquisition planning and preparation for many crucial needs;
- Lack of clearly communicated acquisition responsibilities among FEMA, other federal agencies, and state and local governments; and
- Insufficient numbers of acquisition personnel to manage and oversee contracts.

In February 2006, we reported that FEMA purchased mobile homes without having a plan for how the homes would be used. As a result, FEMA now has thousands of surplus mobile homes. In September 2006, we reported that FEMA spent $7 million renovating a facility to shelter evacuees. Because there was inadequate planning, the facility was never needed. As a result, the facility was underused and the monies spent to renovate were wasted.

FEMA has already made improvements, such as increasing the number of standby contracts in place and ready to be executed when disaster strikes. Also, DHS created a Disaster Response/Recovery Internal Control Oversight Board to address many of the problems. We will soon conduct a review of FEMA's overall acquisition management structure to identify additional improvements that FEMA can make to be prepared better for the next catastrophic disaster. We will review organizational alignments and leadership, policies and procedures, FEMA's acquisition workforce, and its information management. We are also reviewing FEMA's system for accounting for property it has purchased for disasters.

The urgency and complexity of DHS' mission will continue to demand rapid pursuit of major investment programs. While DHS continues to build its acquisition management capabilities in the component agencies and on the department-wide level, the business of DHS goes on and major procurements continue to move. Acquisition management will continue to be an intense area of oversight for our office and an ongoing focus of our audit efforts.

Providing Accurate and Timely Procurement Reporting

In July 2006, we reported on the challenges that DHS faces in planning, monitoring, and funding efforts to ensure the accurate and timely reporting of procurement actions to interested stakeholders. The Executive Branch, the Congress, and the public rely upon such procurement information to determine the level of effort related to specific projects and also to identify the proportion of government contracts that are awarded to small businesses. Currently, however, DHS has several different contract-writing systems that do not automatically interface with its Federal Procurement Data Systems—Next Generation (FPDS-NG)—a government-wide procurement reporting system that is accessible by the public. Some of the systems may need to be replaced. Additionally,

not all DHS procurements are entered into FPDS-NG. For example, grants, mission assignments, and purchase card data may not be entered into FPDS-NG, resulting in an understatement of DHS' procurement activities.

DHS has undertaken a number of initiatives to improve its reporting on procurement actions. These initiatives include interfacing the various DHS contract-writing systems with FPDS-NG and ensuring that all procurement information is entered into FPDS-NG immediately following contract award. Such initiatives will not only enable real-time reporting of DHS procurement actions, they also will allow DHS to rely on General Services Administration databases to help eliminate contract awards to ineligible vendors. The Office of the Chief Procurement Officer has worked with each of the DHS components to improve the accuracy, completeness, and timeliness of FPDS-NG data entry. DHS' planned deployment of a single, contract-writing software system should reduce duplicate data entry for each contract action. DHS is developing routine reporting for non-FPDS-NG instruments.

GRANTS MANAGEMENT

Managing the multitude of grant programs within DHS poses a significant challenge. Further, 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. 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. 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.

Disaster grant awards will be substantially larger than usual with the more than $60 billion that Congress appropriated in late fiscal year 2005 for disaster response and recovery efforts related to 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 the recent 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 fiscal year 2007, DHS is expected to award about $3.4 billion in state and local preparedness grants. We are reviewing individual states' 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 manage effectively and monitor these funds, and to 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.

DHS faces a challenge in addressing its responsibility to become an efficient and effective grants manager. For example, while the Office of Grants and Training is tasked with financial and programmatic monitoring and oversight for first responder grants, the Office of Justice Programs with the Department of Justice does the accounting for these grants. 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.

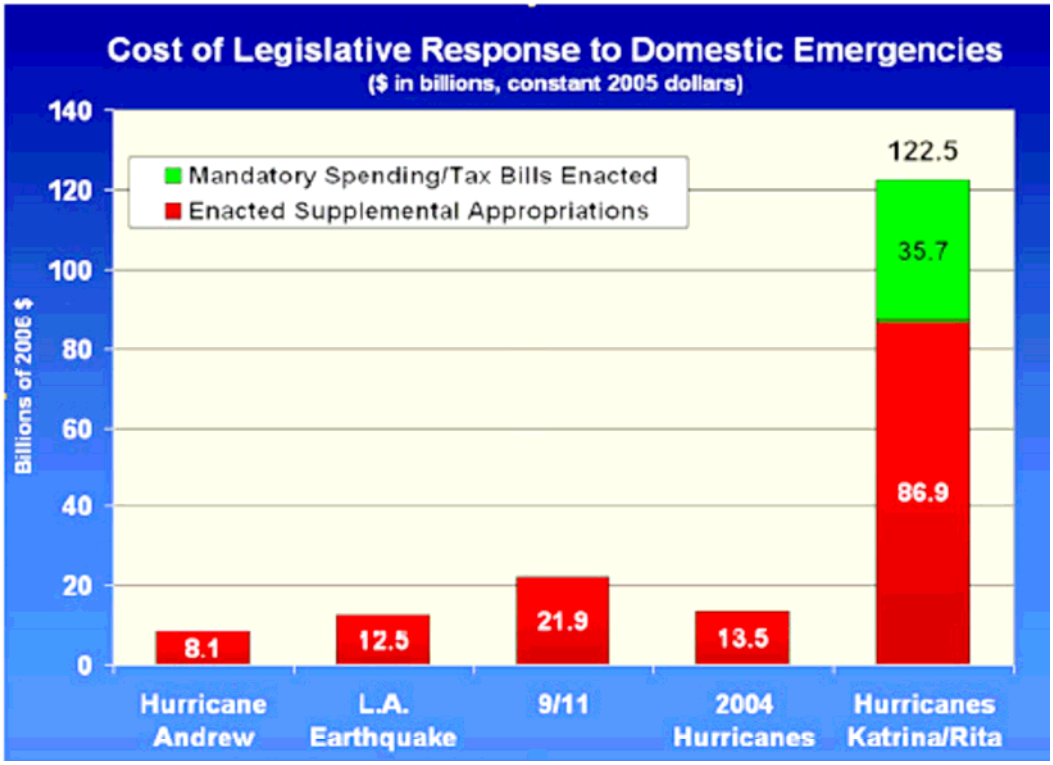
DHS needs to ensure that, to the maximum extent possible, disaster and homeland security assistance go to those states, local governments, private organizations, or individuals eligible to receive such assistance and that grantees adhere to the terms and conditions of the grant awards. DHS needs to continue 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 fiscal year 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.

However, the support for the Gulf Coast hurricanes had a major impact on DHS OIG's nondisaster work, resulting in some delays of audits underway and planned, including the area of grants management. This negative impact was reduced as temporary staff were hired and trained, and employees detailed to Gulf Coast Hurricane Recovery returned to the Office of Audits.

CATASTROPHIC DISASTER RESPONSE AND RECOVERY

In the wake of Hurricane Katrina, Congress responded quickly with funds for immediate relief and recovery efforts. To date, emergency appropriations totaling over $85 billion have been made available. Additionally, Congress enacted over $35 billion in mandatory spending/tax bills, bringing total relief dollars to more than $122 billion.



[Source: Senate Budget Committee, August 22, 2006]

Recognizing the need to protect taxpayers' dollars, the Office of Management and Budget, in early September 2005, mandated that the federal agencies involved in the disaster response and recovery efforts develop a stewardship plan. The plan sets the framework for mitigating risks associated with crisis procurement, managing the broad scope of oversight work, and overseeing contracts awarded.

On the heels of the Office of Management and Budget/Department of Homeland Security plan, the Inspectors General (IGs) involved in oversight of disaster relief efforts developed a hurricane audit coordination model. The model helped determine which recovery activities each of the OIGs would audit and review.

Moreover, the OIG community was well poised to address the need for oversight, as coordination of activities had already been established. Prior to Hurricane Katrina, the President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE) established a Homeland Security Roundtable, based on their collective experience after the 9/11 attacks. The Roundtable was a natural focal point around which hurricane recovery oversight revolved. And, as Chairman of the PCIE's Homeland Security Roundtable, I was tasked with coordinating its activities. Needless to say, Hurricane Katrina oversight was our number one priority last year.

Through the Roundtable, the OIG community has been successful in addressing issues of waste, fraud, and abuse. As of September 30, 2006, through our coordinated activities we have:

- Conducted audits or reviews of 835 contracts, including 348 completed and 487 ongoing audits. These 835 contracts had a total contract value of $8.5 billion. Of this amount, auditors reported questioned costs of $53.6 million, of which $33.3 million was determined to be unsupported.
- Reviewed contracts resulting in $80.9 million in taxpayer funds that could have been put to better use.
- Opened 1,756 cases, which resulted in 439 indictments, 407 arrests, and 255 convictions.

Additionally, in September 2005, I established the Office of Gulf Coast Hurricane Recovery to take the lead in coordinating disaster-related activities. I also appointed a separate Special Inspector General for Gulf Coast Recovery. This action allowed us to stay current on all disaster relief operations, and provide on-the-spot advice on internal controls and precedent-setting decisions.

In turn, the lesson we learned from our experiences in Katrina oversight is that the presence of an office directly responsible for disaster assistance is essential. Therefore, in October 2006, we established the Office of Disaster Assistance Oversight (DAO) to take over, on a permanent basis, the work of the Office of Gulf Coast Hurricane Recovery. I also appointed a permanent Deputy Inspector General for Disaster Assistance Oversight.

The creation of the DAO has strengthened our ability to react quickly and efficiently to a variety of disasters, and further advance our collaborative efforts with other federal IGs. DAO also coordinates the work of the 23 other federal IGs involved in the PCIE Roundtable; actively participates on the Department of Justice's Hurricane Katrina Fraud Task Force; and works closely with state and local auditors and inspectors general, as well as the Government Accountability Office.

The DAO organizational structure to a great extent mirrors FEMA's structure with offices addressing Response, Recovery, Mitigation, and Acquisition. We have three field offices located in Oakland, California, Denton, Texas, and Atlanta, Georgia. Additionally, we have four suboffices co-located or near FEMA's Transitional Recovery Offices, which allow us to work closely with state and local auditors and inspectors general, as well as FEMA regional staff, in order to take a hands-on approach to our oversight efforts. With a total staff of 120 personnel exclusively dedicated to disaster oversight, our structure allows us to be efficient and effective, and to give counsel to address immediate oversight needs. As we continue into the recovery phase of the disaster, we are changing our oversight focus from immediate recovery to acquisition and contract management.

Overall, the work completed by the Gulf Coast Hurricane Office and the DAO has been successful. However, in order to conduct the needed oversight of FEMA's readiness, preparation, response, and recovery related to Hurricane Katrina, we have had to substantially reallocate our inspectors, auditors, and evaluation resources.

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

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.

# # #