DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Major Management Challenges Facing the Department of Homeland Security

(Excerpts from the FY 2007 DHS Annual Financial Report)

OIG-08-11

January 2008

Office of Inspector General

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

Homeland Security

January 4, 2008

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (*Public Law 107-296*) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

The attached report presents the major management challenges facing the Department of Homeland Security and was included in DHS' FY 2007 Annual Financial Report. As required by the Reports Consolidation Act of 2000, we update our assessment of management challenges annually.

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

Richard L. Skinner
Inspector General

Office of Inspector General

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

MAJOR MANAGEMENT CHALLENGES FACING THE DEPARTMENT OF HOMELAND SECURITY

Since its inception in March 2003, the Department of Homeland Security (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 we identify facing DHS, including department-wide and operational challenges, are a major factor in setting our priorities for audits, inspections, and evaluations of DHS programs and operations. As required by the *Reports Consolidation Act of 2000*, Pub.L.No. 106-531, we update our assessment of management challenges annually. We have made recommendations in many, but not all, of these areas as a result of our reviews and audits of departmental operations. Where applicable, we have footnoted specific reports that require DHS' action.

The major management challenges we identified are:

- Catastrophic Disaster Response and Recovery
- Acquisition Management
- Grants Management
- Financial Management
- Information Technology Management
- Infrastructure Protection
- Border Security
- Transportation Security
- Trade Operations and Security

CATASTROPHIC DISASTER RESPONSE AND RECOVERY

Reports issued by the White House, Congress, federal offices of Inspector General, the Government Accountability Office (GAO), and others, have identified longstanding problems within the federal government to sufficiently mobilize a coordinated response operation in the event of a catastrophic disaster. The Department of Homeland Security's (DHS) failures after Hurricane Katrina ravaged the Gulf Coast illuminated a number of these issues, including questionable leadership decisions and capabilities, organizational failures, overwhelmed response and communications systems, and inadequate statutory authorities. In the two years since Hurricane Katrina, a number of federal agencies, private sector organizations, and public offices have issued reports addressing the Federal Emergency Management Agency's (FEMA) weaknesses in response to Katrina.

Additionally, Congress enacted six statutes that contain changes that apply to future federal emergency management actions. Most of the statutes contain relatively few changes to federal authorities related to emergencies and disasters. The Post-Katrina Emergency Management Reform Act of 2006 (Post-Katrina Act), Pub.L.No. 109-295,[1] however, contains many changes that will have long-term consequences for FEMA and other federal entities. That statute reorganizes FEMA, expands its statutory authority, and imposes new conditions and requirements on the operations of the agency. Although FEMA finds itself in a better position today than it did two years ago, it has not fully implemented the Post-Katrina Act. Many of the changes made as a result of the Act, as well as planned response capabilities for future catastrophic disasters, remain untested.

Many problems plaguing FEMA have existed for years, but they never received the attention needed to fix them because FEMA had never before dealt with such a devastating disaster. We are currently in the process of completing audits and reviews to help FEMA turn lessons learned into problems solved and are planning additional work in FY 2008 to assess FEMA's readiness to respond to future catastrophic disasters.

DHS' and FEMA's major management challenges in preparing to meet future catastrophic disasters relate to the following areas: (1) coordination of disaster response efforts, (2) catastrophic planning, (3) logistics, (4) acquisitions, (5) housing, and (6) evacuation. These six critical areas are discussed in detail below.

Coordination of disaster response efforts. When a catastrophic event occurs, disaster response and recovery efforts are not solely a FEMA responsibility – they are inherently the nation's responsibility. Therefore, a successful response to and subsequent recovery from a catastrophic event can be tied directly to the resources and capabilities of citizens, local and state governments, the federal government, nongovernmental organizations, and the private sector. FEMA is the face of our nation's response to large-scale disasters and is charged with coordinating the deployment of our nation's resources and capabilities, but success can only be realized when all stakeholders are fully prepared and willing to contribute.

[1] Post-Katrina Emergency Management Reform Act of 2006 (Post-Katrina Act) Pub.L.No. 109-295, Title VI, 120 Stat.1394.

FEMA's initial response to Hurricane Katrina was significantly impeded by the adjustments it was making in implementing its responsibilities under DHS' National Response Plan (NRP), which was published in December 2004. Moreover, DHS had previously published the National Incident Management System (NIMS) in March 2004. The NIMS, along with the NRP, restructured how federal, state, and local government agencies and emergency responders conduct disaster preparation, response, and recovery activities. Changes needed to implement both plans, however, were still underway when Hurricane Katrina made landfall. Unfortunately, two years later, DHS and FEMA have yet to finalize and issue the National Response Framework, the successor to the NRP, mandated in Title VI of the Post-Katrina Act. Notwithstanding that FEMA provided record levels of support to Hurricane Katrina victims, states, and emergency responders, the response to Katrina demonstrated areas where FEMA and DHS headquarters must make adjustments relating to the use of incident designations, the role of the Principal Federal Official, and the responsibilities of emergency support function coordinators.

Since FEMA is responsible for providing the necessary emergency management leadership to other federal departments, agencies, and other organizations when responding to major disasters, it is largely dependent on other agencies and outside resources to execute many activities that take place. Therefore, departments and agencies need to allocate personnel and funding to train, exercise, plan, and staff disaster response activities to enable better execution of their roles and responsibilities and plans and procedures. Specific contingency plans must be developed and integrated so that capabilities and gaps are identified and addressed.

Hurricane Katrina also highlighted the need for data sharing among federal agencies following a catastrophic disaster. However, data-sharing arrangements between FEMA and other federal agencies to safeguard against fraud and promote the delivery of disaster assistance are not in place. Critical tasks, from locating missing children and registered sex offenders to identifying duplicate assistance payments and fraudulent applications, have all been hindered because mechanisms and agreements to foster interagency collaboration did not exist prior to Hurricane Katrina.

Catastrophic Planning. Attempts to plan for an event such as Hurricane Katrina had been ongoing since 1998, but were never completed for a variety of reasons, including a lack of federal funding, other natural disasters occurring, and the terrorist attacks of September 11, 2001. According to FEMA officials, the major challenge in conducting catastrophic planning is the lack of funding. The GAO reported that requests from FEMA for $100 million for catastrophic planning and an additional $20 million for catastrophic housing planning in fiscal years 2004 and 2005, respectively, were denied by DHS.[2]

The integration of FEMA all hazards preparedness and disaster response and recovery capabilities within DHS requires additional attention. Although an "all-hazards" approach can address preparedness needs common to both man-made and natural events, DHS must ensure that all four phases of emergency management – preparedness, response, recovery, and mitigation – are managed throughout the department on an all-hazards basis. Coordination and

[2] *Hurricanes Katrina and Rita: Unprecedented Challenges Exposed the Individuals and Households Program to Fraud and Abuse; Actions Needed to Reduce Such Problems in the Future,* GAO-06-1013, September 2006.

consultation among DHS components and with state and local governments is essential to guide, advise, develop, and monitor all-hazards capabilities and responder effectiveness.

Planning and exercises also are critical to prepare for and respond to catastrophic events. FEMA recognized the need for catastrophic planning and requested resources for a number of scenarios, including earthquakes in California and along the New Madrid Seismic Zone, hurricanes along the gulf coast, and terrorist attacks. While Congress has appropriated $20 million recently for catastrophic planning, to be successful, FEMA needs to plan and conduct exercises with its federal, state, and local partners. FEMA needs to continue to develop plans and exercises for high risk scenarios and include all its emergency management partners.

Logistics. FEMA is responsible for coordinating the delivery of commodities, equipment, personnel, and other resources to support emergency or disaster response efforts, and therefore, FEMA's ability to track resources is key to fulfilling its mission. In response to Hurricane Katrina, state officials expressed frustration with the lack of asset visibility in the logistics process. FEMA used an inconsistent process involving multiple, independent computer and paper-based systems, many of which generated numerous, unique tracking numbers and few of which were cross-referenced. A White House report revealed a highly bureaucratic federal supply process that was not sufficiently flexible or efficient to meet requirements, and that failed to leverage the private sector and 21st Century advances in supply chain management.

After Hurricane Katrina, FEMA's Logistics Inventory Management System (LIMS) did not track essential commodities, such as food and water. As a result, FEMA could not readily determine its effectiveness in achieving DHS' specific disaster response goals or whether there was a need to improve the system. FEMA's disaster response culture has supported the agency through many crisis situations, such as the 2004 hurricanes. However, FEMA's reactive approach encourages short-term fixes rather than long-term solutions, contributing to the difficulties it encountered in supporting response and recovery operations after Hurricane Katrina. Without taking the time to fully define and document systems requirements, it is difficult for FEMA to evaluate viable alternatives to its custom-designed systems. Also, the reactive manner in which information technology systems are funded and implemented has left little time for testing before they are deployed.

In 2004, FEMA Logistics began testing a total asset visibility pilot program that involved putting tracking units on selected trucks to monitor their movement. In response to Hurricane Katrina, FEMA could only equip about one third of the trucks with tracking units because funds were not available to purchase units for all trucks. In addition, FEMA could not determine whether a truck had been offloaded or had changed cargo once it left its point of origin because of software limitations of the equipment.

Another logistics issue is the use of mission assignments. In response to of Hurricane Katrina, FEMA issued approximately 2,700 mission assignments totaling about $8.7 billion to other federal agencies to acquire goods and services needed for disaster response activities. Historically, FEMA's guidance on mission assignments has been vague and agencies' accounting practices have varied significantly. As a result, FEMA has had difficulty issuing, tracking, monitoring, and closing mission assignments and reconciling agencies' records to FEMA records. FEMA has developed new pre-defined mission assignments to streamline some

of the initial recurring response activities. In addition, FEMA's Disaster Finance Center is working with other federal agencies on appropriate supporting documentation for billings.

Since Hurricane Katrina, FEMA has identified five major commodity storage sites for water, meals, tarps, sheeting, blankets, cots and generators, and has expanded its asset visibility to all regions. Reporting capabilities have been enhanced to allow for more comprehensive and real time reporting from the field. FEMA has interagency agreements with key partners at the Defense Logistics Agency, U.S. Army Corps of Engineers, the Department of Transportation, and the American Red Cross, and is pursuing one with the General Services Administration, to sustain efforts at 100 percent of requirements within 72 hours. These interagency agreements will provide FEMA with essential disaster response commodities, such as meals-ready-to-eat, fuel, ice, medical supplies, water, cots, blankets, tarps, and rental equipment. Each agency will be responsible for tracking its assets and working closely with FEMA and its total asset visibility staff.

Because it is essential to its mission to track assets real-time across federal, state, and local organizations, FEMA has made improvements to LIMS, and has called on the expertise of the private sector to improve total asset visibility. The actions to improve logistical capability are steps in the right direction. Recent events, including the Kansas tornado, indicate improvements in FEMA's response and logistics capabilities. However, whether these improvements will work for a catastrophic event are largely untested.

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 (1) sufficient acquisition planning and preparation for many crucial acquisitions needed immediately after the disaster; (2) clearly communicated acquisition responsibilities among FEMA, other federal agencies, and state and local governments; and (3) sufficient numbers of acquisition personnel to manage and oversee contracts.

Pursuant to the Post-Katrina Act, FEMA has undergone significant reorganization, including in its acquisition function. Major concerns for the acquisition program include the need for: (1) an integrated acquisition system; (2) a full partnership of FEMA's acquisition office with other functions; (3) comprehensive program management policies and processes; (4) appropriate staffing levels and trained personnel; (5) reliable and integrated financial and information systems; and (6) 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 pre-negotiated or "readiness" contracts in advance of disasters;
- Working with DHS' Disaster Response/Recovery Internal Control Oversight Board to address response problems; and

- Continuing its aggressive hiring of highly trained acquisition professionals.

Despite these positive steps, a number of acquisition readiness concerns remain, including the following:

- FEMA has yet to finalize an established process to ensure that federal pre-negotiated contracts for goods and services are coordinated with federal, state, and local governments;

- FEMA has not fully strategized and identified the goods and services for which pre-negotiated contracting may be needed in a catastrophic event; and

- FEMA and other federal agencies may not have enough trained and experienced acquisitions personnel to manage and oversee the vast number of acquisitions that follow major and catastrophic events.

Housing. Possibly the largest problem FEMA faced in the aftermath of Hurricane Katrina was providing financial assistance, sheltering, and housing to evacuees. Because FEMA lacked a catastrophic disaster housing strategy and had never before been faced with meeting the short- and long-term housing needs of hundreds of thousands of disaster victims, it relied on shelters, hotels, motels, cruise ships, and tents, as well as any other available housing resources to meet sheltering and housing needs. FEMA also worked with the Department of Housing and Urban Development (HUD) to implement additional programs to provide housing assistance vouchers to eligible disaster victims. After approximately two years, FEMA has executed an Interagency Agreement with HUD to handle long-term Gulf Coast housing issues.

FEMA's existing programs were inadequate to handle the magnitude of housing requirements after Hurricane Katrina. Also, the number of victims overwhelmed FEMA's system for verifying victim identities and providing individual assistance payments. Consequently, FEMA lessened system controls to accelerate individual assistance payments, resulting in widespread fraud. While FEMA subsequently improved its intake process and the system's capacity, the changes remain untested.

FEMA's efforts to house victims in travel trailers and mobile homes were not well planned, coordinated, or managed, and some outcomes were not anticipated. FEMA purchased mobile homes without a plan for how the homes would be used. As a result, FEMA now has thousands of surplus mobile homes.

The Post-Katrina Act requires FEMA to develop a National Disaster Housing Strategy. The strategy will focus on sheltering, interim and permanent housing, and the various populations to be served, and will guide FEMA and other federal agencies during disasters. The strategy also will identify gaps, such as additional authorities required to deal with sheltering and housing operations, as well as provide flexibility and scalability to meet the unique needs of individual disasters. FEMA has coordinated with other federal agencies and the National Council on Disability to develop a strategy to address housing needs for future disasters. The strategy

includes a Joint Housing Task Force that consists of other federal agencies, state, local, tribal governments, and volunteer agencies. The task force will convene immediately after a Presidential disaster declaration to work with FEMA to coordinate resources and implement housing programs. However, FEMA is looking to other federal and state partners to take a bigger role in disaster housing.

While lessons learned from Hurricane Katrina have improved housing coordination, FEMA needs to develop and test new and innovative catastrophic disaster housing plans to deal with large-scale displacement of citizens for extended periods. Traditional housing programs for non-traditional disaster events have been shown to be inefficient, ineffective, and costly.

Evacuations. Lessons learned from Hurricane Katrina have caused FEMA to take a more active role in evacuating victims during major and catastrophic disasters. While the Department of Transportation has retained responsibility for some transportation functions, FEMA has taken over the standby contracts for air/bus/rail support when state and local governments cannot handle the evacuation process. FEMA is also working closely with states to ensure that evacuation plans are in place. It is critical that FEMA and its federal partners coordinate with state and local governments since catastrophic disaster events will likely exceed their capabilities to handle mass evacuations.

Hurricane Katrina resulted in the activation of Emergency Support Function ESF-6 (Mass Care) with FEMA as coordinator. Because roles and responsibilities were not clearly defined or established, FEMA found it difficult to identify the number and location of evacuees, as well as the need for shelters. The American Red Cross (ARC) stated it was responsible only for coordination and reporting on ARC mass care operations, while FEMA said it relied heavily on ARC to coordinate mass care operations and reporting. The mass care failings after Hurricane Katrina resulted in the development of the National Sheltering System, which is nearly complete. The system, although untested, should allow FEMA to more easily track victims once they arrive at a shelter.

Evacuation plans are complex and must consider a number of scenarios. Recent reports indicate that despite warnings and mandatory evacuation orders, a significant number of individuals will not leave their homes. Others may not be able to evacuate because of health considerations or lack of transportation. State and local officials are in the best position to develop evacuation plans based on these considerations and on local demographics. However, these officials must work closely with FEMA and its federal partners to minimize the loss of life that can result from catastrophic events such as Hurricane Katrina.

ACQUISITION MANAGEMENT

Balancing Urgency and Good Business Practices

With DHS annually spending about 39 percent 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.

We have conducted audits and reviews of individual DHS contracts, such as the U.S. Coast Guard's (Coast Guard) Deepwater program and Customs and Border Protection's (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.

A performance-based acquisition strategy to address the challenges of DHS' 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, 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.[3] 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 recently published the first of what will be a series of scorecards identifying the progress made in selected acquisition functions and activities within DHS.[4] 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. 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.

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

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.

Recent congressional testimony, audits, and reviews indicate deficiencies and the need for DHS to improve all five elements, such as (1) lack of strong acquisition authority in the Office of the Chief Procurement Officer and less than full partnership with other departmental functions; (2) lack of comprehensive program management policies and processes; (3) ineffective internal control over financial reporting; (4) insufficient program management staffing; and (5) 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 are 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 (COTR) 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. During fiscal year 2006, the Under Secretary for Management established policies for acquisition oversight and directed the eight contracting offices 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. 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 percent of DHS' contracting officers will be eligible to retire within the next five 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.[5] The Deepwater acquisition strategy is a non-traditional 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.

Over the past year, the OIG, the GAO, the Defense Acquisition University, and Acquisitions Solutions, Inc. have conducted audits and studies of the Coast Guard's Deepwater Program. These reviews have identified a number of management challenges and risks with the Deepwater Program which raise fundamental questions about the viability of the Coast Guard's "System of System" strategy for re-capitalizing and upgrading its Deepwater fleet of small boats, patrol boats, cutters, helicopters, and fixed-wing aircraft. These challenges and risks include:

- A contract structure that did not easily adapt to the environment of changing missions and requirements, and major systems integration;
- A Deepwater Executive Officer who did not exercise his oversight authority and, as a result, relied on a lead systems integrator to manage the Deepwater program;
- A contract structure that inhibited the Coast Guard's ability to exercise an appropriate level of technical oversight over the acquisition of key Deepwater assets and systems;
- A Deepwater acquisition work force that lacks the requisite training, experience, certification, and structure to acquire assets and systems of significant scope and complexity;
- The Coast Guard's unwillingness 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.

As a result of these and other Deepwater problems, the Coast Guard:

- Discontinued design work on the Fast Response Cutter due to the failure of the contractor to meet minimum design and performance requirements;

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

- Withdrew eight 123-foot patrol boats from service due to the contractor's failure to meet minimum design, construction, and performance requirements outlined in the Deepwater contract; and

- Authorized the expenditure of $1.6 billion to construct three National Security Cutters with the knowledge that the cutter, as currently designed, had structural design flaws that prevent it from meeting the mission performance requirements outlined in the Deepwater contract.

To its credit, the Coast Guard now recognizes the need for urgent and immediate changes to the way it manages its major acquisitions in general, and the Deepwater Program in particular. For example, the Coast Guard recently issued its *Blueprint for Acquisition Reform*, July 13, 2007 (Blueprint), which catalogues many of the aforementioned challenges and risks that have historically impeded the efficient execution of the Deepwater contract acquisition projects. According to the Coast Guard, implementing this Blueprint will enhance its ability to efficiently execute asset-based "traditional" projects, effectively employ a governmental or commercial entity as a systems integrator for complex acquisitions, and efficiently execute non-major acquisitions and contracts for necessary goods and services.

The Blueprint specifically outlines the Coast Guard's plans for reorganizing its acquisition workforce, an effort that is expected to take several years and an unknown amount of money to implement. The Blueprint, however, does not contain critical measures of performance that would allow the Department and the Congress to assess the progress being made. For example, the Blueprint does not describe the number and type of acquisition professionals needed or when they are scheduled to arrive on board.[6] In addition, while the Blueprint contains a number of key initiatives, it does not clearly state the outcomes that will be achieved, and at what cost to the Coast Guard. Finally, neither the Blueprint nor the Coast Guard has identified the changes to the Deepwater contract that will be made to ensure full implementation of the Blueprint. Consequently, it is difficult to determine whether these initiatives will satisfactorily address the cost, schedule, and performance issues associated with the Deepwater 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 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.

[6] Major systems acquisition competency areas that are in the greatest need of infusion of experience are program management, contracting, and financial management (including earned value management and cost estimating). Defense Acquisition University, *Quick Look Study, United States Deepwater Program*, February 2007.

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 Emergency Management Reform Act of 2006, the grant programs administered by the Office of Grants and Training transferred to the 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 Grants Program 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). 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 percent 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. The FEMA Integrated Financial Management Information System (IFMIS) will be the key financial reporting system, which has feeder subsystems for budget, procurement, accounting and other administrative processes and reporting. For the short-term, FEMA will run two financial systems: (1) FEMA IFMIS, and (2) Grants and Training IFMIS. This will allow FEMA to incorporate all Grants and Training financial data, including grants data, within the new FEMA. Grants and Training IFMIS includes grantee payment functionality and financial status reporting capabilities. In FY 2008, Grants and Training IFMIS data will migrate to FEMA IFMIS 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 $110 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.[7]

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

[7] DHS OIG: *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.

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.

FINANCIAL MANAGEMENT

Financial management has been a significant challenge for DHS since its creation in 2003. This year, the independent auditors, KPMG LLP (KPMG), under contract with the OIG will be unable again to complete an audit of the DHS consolidated balance sheet and Statement of Custodial Activity as of and for the year ended September 30, 2007. In addition, KPMG noted that numerous material weaknesses in internal control continued to exist. However, the majority of the department's material weaknesses in internal control are attributable to conditions existing at the Coast Guard.

The material weaknesses in internal control are impediments to obtaining an unqualified opinion and have precluded management from giving positive assurance over internal control at the department level.[8] DHS' ability to obtain an unqualified audit report and provide assurances that its system of internal control is designed and operating effectively, is highly dependent upon process and procedural improvements at the Coast Guard, Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), FEMA and OCFO.

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 FY 2006, DHS took the initial step in this process by preparing comprehensive corrective action plans to address known internal control weaknesses. The corrective actions plans from each component were incorporated into a single management strategy document identified as the Internal Control Over Financial Reporting 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.

Consequently, during FY 2007, we anticipate that DHS will make 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 early in the second quarter of FY 2008. Further, conditions reported as material weaknesses in internal control in previous independent auditor reports will be updated and reported in the DHS Performance and Accountability Report, submitted to the Office of Management and Budget on or before November 15, 2007. The

[8] DHS-OIG, *Independent Auditors' Report on DHS' FY 2006 Financial Statements*, OIG-07-10, November 2006.

independent auditor report will include specific conditions and recommendations for DHS consideration in updating its corrective actions in FY 2008.

INFORMATION TECHNOLOGY MANAGEMENT

Integrating the information technology (IT) systems, networks, and capabilities of the various legacy agencies to form a single infrastructure for secure, effective communications and information exchange remains one of DHS' biggest challenges. There are multiple aspects to achieving such an IT infrastructure. For example, creating an adequate capability for relocating mission critical information systems to an alternate disaster recovery site in the event of extended service disruptions or emergency is one concern. Implementing a department-wide program that ensures effective information security controls and addresses IT risks and vulnerabilities is just as key. Further, improved IT planning, requirements identification, and analysis will be essential not only to acquire and implement the systems and other technologies needed to streamline operations within individual DHS component organizations, but also to support effective homeland security information sharing with state and local governments, the private sector, and the public. Without sound department-wide planning, coordination, and direction, the potential for integrating advanced data mining functionality and capabilities to address homeland security issues will remain untapped also. Finally, DHS faces a major challenge in addressing privacy concerns while integrating its myriad systems and infrastructures.

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 will 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.

Security of IT Infrastructure

The security of IT infrastructure is a major management challenge. As required by the *Federal Information Security Management Act* (FISMA), the CIO must develop and implement a department-wide information security program that ensures the effectiveness of security controls over information resources, including its intelligence systems, and addresses the risks and vulnerabilities facing DHS' IT systems.

As we reported in September 2007, based on its annual FISMA evaluation, excluding its intelligence systems, DHS continues to improve and strengthen its security program.[9] DHS implemented a performance plan to measure the 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 FISMA evaluations, during the past year we conducted information security audits of DHS laptop computers, performed technical security evaluations at Ronald Reagan Washington National Airport and Dulles International Airport, 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.

[9] DHS-OIG, *Evaluation of DHS' Information Security Program for Fiscal Year 2007*, OIG-07-77, September 2007.

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: (1) certification and accreditation; (2) vulnerability testing and remediation; (3) contingency plan testing; (4) incident detection, analysis, and reporting; (5) security configurations; and (6) 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.

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 follow-up review that U.S. Citizenship and Immigration Services (USCIS) had 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.[10] 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 will not be in a position to either effectively manage existing workloads

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

or handle the potentially dramatic increase in immigration benefits processing workloads that could result from proposed immigration reform legislation.

Similarly, our December 2006 follow-up 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 (EA), 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 2006 hurricane season and made little progress in addressing long-term needs, such as updating strategic plans, defining cross-cutting requirements, and evaluating systems alternatives.

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.[11] 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.[12] 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

[11] DHS-OIG, *ADVISE Could Support Intelligence Analysis More Effectively*, OIG-07-56, June 2007.
[12] DHS-OIG, *Better Management Needed for the National Bio-Surveillance Integration System Program*, OIG-07-61, July 2007.

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.

Privacy

DHS collects large amounts of information to support its various missions, and much of this information is personal, and must be protected in accordance with federal statutes governing privacy. As such, DHS faces challenges in ensuring that privacy concerns are addressed throughout the lifecycle of each information system or program. Our reviews of DHS programs have identified instances where DHS' efforts to meet these challenges are falling short.

Specifically, following several recent incidents involving the compromise or loss of sensitive personal information, Office of Management and Budget (OMB) issued Memorandum 06-16 *Protection of Sensitive Agency Information* on June 23, 2006. The memorandum recommends measures to compensate for the lack of physical security controls when information is removed from or accessed from outside the agency location. These measures include (1) verifying the adequacy of agency policies and procedures; (2) identifying systems processing Personally Identifiable Information (PII); (3) encrypting data on laptops and mobile computing devices; and (4) implementing remote access security and offsite transportation and storage controls.

In November 2006, we reported on DHS' implementation of the recommendations set forth in OMB Memorandum 06-16. We noted that DHS and its components are in the process of implementing OMB's recommended security controls for sensitive data and PII. DHS has issued updated policies and procedures to address OMB's recommendations. Further, DHS is in the process of identifying PII systems, encrypting laptop computers, and implementing remote access security and offsite transportation and storage controls. Until all systems collecting, processing, or storing PII are identified, and adequate controls for protecting remote access and storage of PII are implemented, DHS lacks assurance that sensitive data are properly protected.

In addition, our June 2007 report on ADVISE stated that S&T program management did not begin the privacy impact process until after several pilots for the ADVISE program were already operational.[13] Federal agencies are required to conduct a Privacy Impact Assessment for each new or substantially changed IT system that collects, maintains, or disseminates personally identifiable information. For its part, the DHS Privacy Office did not know that S&T had proceeded with implementation of the ADVISE pilot programs with live data, but without addressing privacy matters. In a July 6, 2006, report to the Congress, the Privacy Office stated that the ADVISE tool alone does not perform data mining. However, the report went on to explain that implementation of this system with live data could be considered a data mining tool. Unbeknownst to the Privacy Office, the ADVISE pilots had been implemented at least 18

[13] DHS-OIG, *ADVISE Could Support Intelligence Analysis More Effectively*, OIG-07-56, June 2007.

months prior to its July 2006 report. Failure to properly address privacy issues prior to deploying the three pilots had the ultimate effect of bringing the ADVISE program to a halt.

Finally, our July 2007 report on the National Bio-Surveillance Integration System program (NBIS) revealed that DHS officials did not effectively coordinate with federal stakeholders to address concerns about the privacy and security of data shared.[14] Without NBIS program officials first defining what information NBIS needs, stakeholders had little basis to determine what information might be released by their agencies.

Information Sharing

The *Homeland Security Act of 2002*[15] 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 user communities in developing the system.[16] 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 a 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 are 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.[17] For example, CBP performs matching 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

[14] DHS-OIG, *Better Management Needed for the National Bio-Surveillance Integration System Program*, OIG-07-61, July 2007.
[15] P.L. 107-296.
[16] DHS-OIG, *Homeland Security Information Network Could Support Information Sharing More Effectively*, OIG-06-38, June 2006.
[17] DHS-OIG, *Survey of DHS Data Mining Activities*, OIG-06-56, August 2006.

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.

INFRASTRUCTURE PROTECTION

DHS is responsible for coordinating the national effort to enhance protection of critical infrastructure and key resources (CI/KR) of the United States. Specifically, DHS has direct responsibility for leading, integrating, and coordinating 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. In addition, DHS has an oversight role in coordinating the protection of CI/KR for which other federal agencies have the primary protection responsibility. Those CI/KR include agriculture and food; the defense industrial base; energy; public health and healthcare; national monuments and icons; banking and finance; and water and water treatment systems. Combined with the uncertainty of the terrorist threat and other manmade or natural disasters, the effective implementation of protection efforts is a great challenge.

DHS has numerous CI/KR responsibilities to discharge. After issuing the National Infrastructure Protection Plan in June 2006, DHS worked toward completion of specific plans for each critical infrastructure sector. On May 21, 2007, the DHS Secretary approved all 17 sector-specific plans. More work needs to be done in the different sectors. For example, in the chemical sector, DHS issued an Interim Final Rule for Chemical Facility Anti-Terrorism Standards in April 2007. The department is now completing the rule, ensuring that vulnerability assessments are conducted, and fostering the development of site security plans. In the transportation sector, DHS is working to establish a Sector Coordinating Council and implement new statutory requirements. In the agriculture and food sector, we reported that DHS has satisfied most of its basic requirements but still needed to submit an integrated federal food defense budget plan and clearly establish assessment standards for use in the food sector.[18]

The nation's CI/KR distribution is enormous and complex. The requirement to rely on the private sector and federal partners to deter threats, mitigate vulnerabilities, or minimize incident consequences complicates protection efforts for all CI/KR. We reported several opportunities for DHS to improve its engagement of public and private partners.[19] DHS also could do more to prioritize resources and activities based on risk. To assist in overcoming this great challenge, the National Infrastructure Protection Plan envisions a comprehensive, national inventory of assets, known as the National Asset Database (NADB), to help carry out these responsibilities. A maturing NADB is essential to the development of a comprehensive picture of the nation's CI/KR, as well as to management and resource allocation decision-making. As we reported in FY 2006, DHS is improving the development and quality of the NADB.[20] DHS also is

[18] DHS OIG, *The Department of Homeland Security's Role in Food Defense and Critical Infrastructure Protection*, OIG-07-33, February 2007.
[19] DHS OIG, *Review of the Buffer Zone Protection Program*, OIG-07-59, July 2007; *The Department of Homeland Security's Role in Food Defense and Critical Infrastructure Protection*, OIG-07-33, February 2007.
[20] DHS OIG, *Progress in Developing the National Asset Database*, OIG-06-40, June 2006.

strengthening its relationships with other responsible federal departments. Standardizing vulnerability assessment methodologies, such as the Risk Analysis and Management for Critical Asset Protection tool, will also help the department better understand CI/KR.[21]

We will continue to monitor and review how DHS coordinates infrastructure protection with other sectors, how it uses the NADB to support its risk management framework, and how its pursuit of basic vulnerability assessment standards can help develop overarching departmental priorities.

Protecting the nation's cyber infrastructure also is a challenge for DHS. Since our last review in 2004, the National Cyber Security Division has taken actions to further implement *The National Strategy to Secure Cyberspace* that was published by the White House in February 2003. For example, the division has established a fully operational incident handling center (United States Computer Emergency Readiness Team). The National Cyber Security Division has put into action programs that promote cyber security awareness among the public and private sectors; improve vendor software development and reduce vulnerabilities; develop and promote sound practices and standards that enhance cyber security; promote a global culture of security through international outreach awareness; promote and facilitate the development of adequately trained IT professionals; and plan, coordinate, and conduct cyber exercises with the public and private sectors to improve cyber security readiness, protection, and incident response capabilities. The National Cyber Security Division has established working groups and participated with public and private sector organizations to share information and protect cyberspace and cyber assets.

While the National Cyber Security Division has made progress in meeting its mission, it can improve its efforts to secure the nation's cyber infrastructure. Specifically, the division has not (1) established priorities to ensure that its mission-critical tasks supporting its programs are completed timely; (2) developed enhanced performance measures that can be used to evaluate effectiveness in meeting its mission; (3) fully developed its information sharing and communications programs with the private sector; (4) developed and implemented enhanced procedures to ensure that all known cyber incidents from across the federal government are reported.

BORDER SECURITY

One of DHS' primary missions is to reduce America's vulnerability to terrorism by controlling the borders of the United States. This mission is shared by a number of agencies within DHS and is dependent on the coordinated accomplishment of each agency's roles as well as, joint efforts with other agencies. To this end, DHS created and is implementing a comprehensive multi-year plan to secure the borders and reduce illegal immigration. This plan, called the Secure Border Initiative (SBI) orchestrates roles for CBP, ICE, CIS, Coast Guard, and other components.

[21] DHS OIG, *A Review of Homeland Security Activities Along a Segment of the Michigan-Canadian Border,* OIG-07-68, August 2007.

This plan should address some of the previously reported challenges. For example, last year we reported that CBP and ICE continue to experience difficulties in coordinating and integrating their respective operations.[22] More than two years after their creation, CBP and ICE have not come together to form a seamless border enforcement program. Their operations have significant interdependencies that have created conflict between CBP and ICE. Jurisdictional, operational, and communication gaps exist between the two organizations that must be addressed by DHS leadership.

Our follow-up review determined that DHS has made significant progress toward improving coordination and interoperability between CBP and ICE. Additional work is needed to: improve communication between headquarters and field elements; share information and intelligence; strengthen performance measures; and address relational issues among some component elements.[23]

Another example is the integration of border surveillance technologies. Previously, we reported that border surveillance cameras were not integrated with ground sensors, and sensors are plagued by false alarms. We recommended that CBP improve the effectiveness of remote surveillance technology.[24]

As previously reported, maintaining a systems approach to addressing the challenge of securing our borders is a major challenge as the SBI focus shifts to the DHS components' implementation of the various plans comprising SBI. The major planned efforts under SBI are led by the three lead components for immigration and border security.

- ICE leads plans to improve the apprehension, detention, and removal of illegal aliens, and to expand worksite enforcement. Improvements in alien detention and removal efforts require coordinated efforts across DHS and collaboration with the Department of Justice and other agencies sharing responsibility for this function.

- CIS leads plans for a temporary guest worker program; streamlining immigration benefits processes; and expanding the employment verification program. CIS plans to focus on automating and improving processes to (1) increase efficiency, (2) alleviate chronic backlogs in benefit application processing and adjudications, and (3) handle anticipated increases in applicants under proposed expanded guest worker initiatives.

- CBP leads a major investment program to gain control of the borders called SBInet. The SBInet objective is to develop solutions to manage, control, and secure the borders using a mix of technology, infrastructure, personnel, and processes. While SBInet is a new program, it replaces two previous efforts to gain control of the borders: the Integrated Surveillance Intelligence System and the America's Shield Initiative. CBP awarded a

[22] DHS-OIG, *An Assessment of the Proposal to Merge Customs and Border Protection with Immigration and Customs Enforcement*, OIG-06-04, November 2005.
[23] DHS-OIG, *DHS' Progress in Addressing Coordination Challenges Between Customs and Border Protection and Immigration and Custom Enforcement*, OIG-07-38, April 2007.
[24] DHS-OIG, *A Review of Remote Surveillance Technology Along U.S. Land Borders*, OIG-06-15, December 2005.

multiple year systems integration contract in September 2006 to begin the SBInet multi-billion 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.[25] The SBI procurement presents a considerable acquisition risk because of its size and scope.

Our main concern about SBInet is that DHS is embarking on this multi-billion dollar acquisition project without having laid the foundation to effectively oversee and assess contractor performance and effectively control cost and schedule. DHS did not properly define, validate, and stabilize 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 is precluded. DHS also needs to move quickly to establish the organizational capacity to properly oversee, manage, and execute the program. In our March 2006 semiannual report, we reported progress in building that capacity and we continue to monitor this program and the new acquisition organizations closely.

Additionally, CBP faces challenges attendant to the rapid build-up of its force structure, especially the significant increases in the number of US Border Patrol Agents. In an effort to secure our nation's border, President Bush announced in May 2006 that the Border Patrol would add an additional 6,000 agents by the end of 2008. With this rapid expansion came several challenges for the Border Patrol, including recruiting, hiring, and training a sufficient number of Border Patrol agents; providing sufficient vehicles for agents; and ensuring that there are adequate facilities to house the number of agents entering on duty. While the Border Patrol has made progress in its expansion efforts, challenges continue to arise in order for the Border Patrol to realize its goal over the next 15 months. To improve recruiting, CBP has developed and implemented a strategic plan to meet its recruiting goals. Ensuring hiring process are supported by effective and timely background checks remains a concern as delays increase and instances of hires subsequently found to be unsuitable occur. In addition, once Border Patrol agents are hired and enter on duty, they are required to attend and complete training at the Border Patrol Academy and, once on station, to receive on-the-job training from experienced agents. The Border Patrol is challenged to maintain the quality of training as it changes the curriculum to accommodate the flow of students and as the ratio of experienced agents to new recruits decreases. Also, there are experienced agents who have the perception that the Academy has relaxed its standards and is graduating agents that are not well trained to meet the challenge of being an agent.

Also, the Border Patrol must ensure that agents have the vehicles necessary to conduct their mission. Vehicles used by Border Patrol agents in 2006 exceeded the recommended life for about half the fleet; however, CBP reported that funds were not available to replace vehicles in FY 2006. In FY 2007 the budget provided for marginal Border Patrol fleet growth, although during the same period the Border Patrol agent count increased by 25 percent.

[25] DHS-OIG, *Risk Management Advisory for the SBInet Program Initiation,* OIG-07-07, November 2006.

Finally, CBP needs to ensure that that there are adequate facilities to accommodate the increase of Border Patrol agents. This includes predicting the location and number of new agents being deployed, building concurrent construction projects, and funding for construction projects. The location and number of new agents to be deployed are key factors in the planning process. Agents are deployed based on operational needs, which can change as the amount and type of activity changes on the border. As agents are redeployed or newly deployed, CBP has to change its real estate to accommodate them. One way CBP responds to this challenge is with Rapid Response Projects. CBP currently is building 73 Rapid Response Projects at the same time. However, building concurrent projects takes a large amount of coordination and communication between CBP and its various service providers. With so many projects underway at one time, CBP may not be able to apply adequate oversight and controls to ensure that schedule, quality, and cost requirements are met. We are reviewing the construction of Border Patrol facilities.

Other DHS components share border security responsibilities and are necessarily part of a comprehensive solution to border and immigration control. For example, the US-VISIT Program is responsible for developing and fielding DHS' entry-exit system. It also coordinates the integration of two fingerprint systems: DHS' Automated Biometric Identification System and the Federal Bureau of Investigation's Integrated Automated Fingerprint Identification System. While US-VISIT has some early accomplishments, the tracking of foreign visitors and immigrants still has weaknesses, especially on exit, that should be addressed under a systems approach.

DHS also needs to address other weaknesses as part of the comprehensive solution to immigration and border control. For example, CBP needs to fuse the intelligence gathered with intelligence requirements to accomplish its priority mission. The CBP mission of preventing terrorists and terrorist weapons from entering the United States, while facilitating the flow of legitimate trade and travel is critical. Differentiating between the two requires timely intelligence. The ability of CBP to gather intelligence information and distribute it to field personnel has a direct effect on security at our borders. Border security also depends on information about terrorists kept on various watch lists. The watch lists are managed by several federal agencies. Those agencies and DHS need to coordinate access to the lists to ensure valuable information flows through CBP to field personnel on the line.

We will continue to maintain an aggressive oversight program for DHS' border security initiatives to ensure that DHS applies a systems approach and carries out the resultant plans and programs in an economical, efficient, and effective manner.

TRANSPORTATION SECURITY

Aviation

TSA was created in the wake of the terrorist attacks of September 11, 2001, to strengthen the security of the nation's transportation systems. The *Aviation and Transportation Security Act* (ATSA),[26] established TSA to protect the nation's transportation system, encompassing aircraft,

[26] P.L. 107-71, November 19, 2001.

ships, rail and motor vehicles, airports, seaports, trans-shipment facilities, roads, railways, bridges, and pipelines from terrorist attacks and criminal activity. TSA employs approximately 50,000 people responsible for:

- Ensuring thorough and efficient screening of all aviation passengers and baggage through an appropriate mix of federalized and privatized screeners and technology;

- Promoting confidence through the deployment of Federal Air Marshals to detect, deter, and defeat hostile acts targeting air carriers, airports, passengers, and crews; managing the security risk to the surface transportation systems in partnership with federal, local, and private stakeholders;

- Developing and implementing more efficient, reliable, integrated, and cost effective terrorist related screening programs; and

- Improving organizational effectiveness by expanding capabilities of the workforce to leverage limited resources.

The size and complexity of the transportation system, which moves millions of passengers and tons of freight every day, makes it a difficult system to secure and an attractive target for terrorists. The nation's economy depends upon implementation of effective, yet efficient transportation security measures. However, since its inception, TSA has focused almost all of its attention on aviation security.

As part of its mandate, TSA has had to recruit, assess, hire, train, and deploy Transportation Security Officers (or TSOs, formerly known as "screeners") for approximately 450 commercial airports, and provide 100 percent screening of all checked luggage for explosives. TSA, originally a part of the Department of Transportation, became part of DHS in March 2003. Transportation security management challenges are as follows:

Checkpoint and Checked Baggage Performance

The ATSA requires TSA to screen or inspect all passengers, goods, and property before entry into the sterile areas of the airport. The OIG has periodically conducted undercover penetration testing to determine to what extent TSA's policies, procedures, equipment, and supervision ensure that TSO performance prevents threat items from entry into the sterile area and the checked baggage systems of the nations airports. Through our periodic testing, the OIG has assessed whether TSA's screening policies and procedures are adequate, whether TSOs follow the screening policies and procedures, and whether aviation security screening equipment and technologies are functioning properly and as intended. Our undercover audits of screener performance revealed that improvements are needed in the screening process to ensure that dangerous prohibited items are not being carried into the sterile areas of heavily used airports and do not enter the checked baggage system. In past testing, we noted four areas that caused most of the test failures and were in need of improvement: training; equipment and technology; policy and procedures; and management and supervision. TSA agreed with our conclusion that significant improvements in screener performance will only be possible with the introduction of

new technology. During FY 2008, we will release a classified report on our latest penetration testing results, including the effectiveness of TSA's performance in implementing newer technologies.

Passenger Air Cargo Security

The vast and multifaceted air cargo system transports approximately 7,500 tons of cargo on passenger planes each day, making air cargo vulnerable to terrorist threats. The Assistant Secretary of TSA has primary responsibility for enforcing and implementing all regulations related to aviation security. TSA enforces statutory and regulatory requirements, disseminates threat-related information, and provides guidance and some funding. TSA relies on the oversight and inspections carried out by Aviation Security Inspectors (ASI), who are located at airports throughout the United States. ASIs are responsible for inspecting approximately 285 passenger and all-cargo air carriers with about 2,800 cargo facilities nationwide. TSA has approximately 300 Cargo ASIs, supplemented by 600 Generalist ASIs, responsible for conducting inspections of screening activities at approximately 100 airports.

Recent OIG work showed that TSA's inspection process might not accurately represent the extent to which air carriers comply with cargo screening requirements. Additionally, TSA does not provide sufficient resources for air carrier inspection coverage. Therefore, ASIs do not have the capability to monitor cargo screening activities and are unable to report accurately on air carrier compliance. TSA's compliance database, the Performance and Results Information System, is ineffective as a tool to monitor and report air carrier compliance with screening regulations. In addition, the current level of oversight does not provide assurance that air carriers are meeting congressionally mandated goals of tripling the amount of cargo screened for passenger aircraft and that air carriers are properly applying exemption rules for cargo screening. Consequently, the process increases the opportunities for the carriage of explosives, incendiaries, and other dangerous devices on passenger aircraft.

Workers' Compensation

The physical activity required to screen passengers and baggage at the nation's airports has resulted in an inordinate number of injuries for TSA screeners. In FY 2007, the OIG completed an audit to determine whether TSA is effectively and aggressively managing its Federal Employees' Compensation Act (FECA) program to reduce workplace injuries, and minimize lost workdays and FECA-related compensation costs by returning work-capable employees to work as soon as possible. We concluded that TSA made substantial progress in improving the timeliness of new injury claims, reducing both the number of workers' compensation claims and lost time associated with workplace injuries. However, TSA must take steps to better manage its workers' compensation caseload. We identified claimants who were receiving long-term compensation for up to three years despite the fact that medical evidence indicated work capability. We also identified claimants who were not offered limited duty when capable and, when permanent restrictions existed, not recommended for vocational rehabilitation in a timely manner. As a result, the agency may be paying benefits to individuals who are not entitled to them, and may be at risk of workers' compensation fraud and abuse. In addition, the agency did not have a process to validate its workers' compensation chargeback reports. Without reviewing its chargeback reports the agency is unable to determine whether the Department of Labor is

accurately billing the agency and is likely incurring inappropriate or excessive costs at other airports nationwide.

We made 12 recommendations to the Assistant Secretary of the TSA to strengthen the controls over its Federal Employees' Compensation Act program. Recommendations included a re-evaluation of long-term cases, more guidance and training for staff, a centralized tracking system for FECA cases, better monitoring of FECA costs, and sharing of safety best practices and incentive programs. TSA generally concurred with the recommendations in the report and has already taken steps to address several of them.

Employee Workplace Issues

A stable, mature, and experienced TSA workforce is the one of the most effective tools the agency has to meet its mission. Since 2004, TSA has been sharply criticized by its employees, primarily TSOs, for alleged discrimination, selective hiring practices, nepotism, management violations, and lax oversight. TSA employees have been voicing their concerns about how the agency operates by filing discrimination complaints that were significantly higher than its closest competitors among federal agencies. TSA has faced high attrition rates and low employee morale, which some say is the result of a lack of employee rights and protections. High levels of workplace dissatisfaction among the TSA screener workforce could compromise organizational stability and, therefore, the effectiveness of airport security operations. In FY 2008, we will issue a report on how effective TSA has been in proactively identifying and addressing employee workplace problems, issues and concerns.

Rail And Mass Transit

Surface transportation systems are extremely vulnerable to terrorist attack, as evidenced by the attacks on passenger rail facilities in Madrid, London, and India. Passenger rail, bus, highway, and ferry systems are inherently difficult to secure in the United States because of their open accessibility (typically, many entry and exit points), high ridership (nearly 9 billion transit trips per year on buses and subways), and extensive infrastructure (roughly 11,000 track miles of transit rail and 3000 stations, 3.8 million miles of roads nationwide, and more than 600,000 bridges and tunnels). While the majority of mass transit systems in the nation are owned and operated by state and local governments and private industry, securing these systems is a shared responsibility among federal, state, and local partners. More robust information exchange, threat detection, and preparedness measures must be undertaken to ensure the security and resilience of the surface transportation system.

The Transportation Sector Specific Plan that DHS published in May 2007 brings together federal, state, and local government partners and regional mass transit stakeholders to create a "a secure, resilient transit system that leverages public awareness, technology, and layered security programs while maintaining the efficient flow of passengers."[27] Nevertheless, the task of prioritizing and securing surface transportation is daunting. DHS has made millions of dollars available through the Transportation Security Grant Program, Homeland Security Grant Program, Trucking Industry Security Grant Program, Urban Area Security Initiative, and other

[27] DHS, *Transportation Sector-Specific Plan: Mass Transit Modal Annex*, May 21, 2007 (page 3).

funding methods. For rail and public transit safety grant programs in particular, the Congress provided $275 million in FY 2007, and FY 2008 funds may exceed $400 million. Other DHS programs include the Surface Transportation Security Inspection Program, in which TSA employs inspectors who assess a transit system's security posture and act as local liaisons. Additionally, TSA trains and deploys supplemental security manpower for high-risk transit systems through Visual Intermodal Protection and Response Teams and provides free explosive detection canines for transit systems through its Canine Program. DHS also develops and tests new technologies, such as more effective chemical and explosive detection equipment, mobile security checkpoints, and video surveillance systems.

We are reviewing DHS actions to improve passenger rail security on subway and commuter rail systems through various TSA programs, assessing how well these programs intersect with federally funded programs operated at the local level. We are examining the impact that the federal grants and policies have on local transit authorities. We also are reviewing the effectiveness of the trucking industry security grant program.

TRADE OPERATIONS AND SECURITY

Trade operations and security primarily are the responsibility of CBP, although USCG and ICE also play important support roles. CBP has the counterbalancing missions of facilitating legitimate trade and enforcing the laws associated with trade and border controls. CBP has the challenge of interdicting smuggling and stopping other illegal activities, that benefit terrorists and their supporters. In a typical year, CBP processes millions of sea containers, semi-tractor trailers, rail cars, and tons of bulk cargo and liquids, such as chemicals, crude oil, and petroleum products. CBP also processes or reviews all of the personnel associated with moving this cargo across U.S. borders or to U.S. seaports.

CBP has implemented a number of initiatives to accomplish this objective such as the Container Security Initiative, and Customs-Trade Partnership Against Terrorism (C-TPAT). CSI works with foreign allies and partners to screen and examine containerized cargo at overseas ports before it is loaded on ships bound for the U.S. The initiative calls for the increased use of non-intrusive technology to inspect this cargo both overseas and at U.S. ports. Within C-TPAT, CBP works with trade representatives to develop and implement processes and systems to help secure the supply chain. CBP uses targeting systems to assist in identifying the highest risk cargo on which to focus its limited resources. Other initiatives include the Secure Freight Initiative, a comprehensive model for improving global supply chain security while keeping legitimate trade flowing. Officially launched on December 7, 2006, it is designed to leverage information, foreign government and commercial partnerships, plus the latest technology to reduce the risk of terrorism.

In support of its trade mission, CBP is undertaking an extensive and long-term effort to develop a new system, Automated Commercial Environment (ACE), to replace older, less effective, and less capable trade processing systems. The ACE Release 4 provides an electronic truck manifest, screens for CBP officers' use, and expedited importation processing. In our 2007 audit, we reported that generally, problems referred to the ACE help desk were resolved effectively. However, CBP did not detect and resolve some operational problems that occurred at the ports

and did not provide adequate communication and guidance to the ports. We recommended that CBP develop procedures to monitor post-deployment operations and communicate ACE problems, operational fixes, and system changes to CBP Officers at the ports in a timely manner.[28]

The Automated Targeting System (ATS) helps CBP identify high-risk cargo for inspection. In 2005, we reported concerns about the data to which ATS targeting rules are applied, the use of examination results to refine ATS targeting rules, and physical controls over cargo containers targeted for examination.[29] In our second ATS report, issued in November 2006, we reported that CBP did not fully utilize other sources of intelligence information available and that national ATS performance measures were still being developed for determining the effectiveness of the ATS. Furthermore, we found that additional guidance for inspection of shipments with elevated ATS scores was needed.[30]

In 2007, we reported that CBP was not consistently using entry data for all shipments, resulting in some high-risk containers being allowed to leave ports without mandatory examinations. Further, flaws in the Cargo Enforcement Reporting and Tracking System may result in improper container releases, and CBP had not automated its integration of examination findings into ATS. Finally, some ports needed to improve controls over high-security bolt seals. CBP concurred with all of the recommendations and subsequent to the end of our fieldwork, took actions to improve procedures for preventing containers from leaving the ports without the required examinations.[31]

In the export arena, our audit concluded that outbound shipments are not consistently targeted and inspected by CBP officers at the ports for compliance with federal export laws and regulations. As a result, shipments could be exported that violate laws and regulations. We made several recommendations to help CBP ensure trade adherence with federal export laws and regulations.[32]

The Coast Guard is the lead DHS agency for maritime homeland security and is responsible for developing and implementing a comprehensive National Maritime Transportation Security Plan to deter and respond to transportation security incidents. The marine areas under U.S. jurisdiction cover 3.5 million square miles of ocean, 95,000 miles of coastline, and 26,000 miles of commercial waters serving 361 domestic ports. These activities account for two billion tons and $800 billion of domestic and international freight annually. Approximately 8,000 foreign vessels, manned by 200,000 foreign sailors, make more than 50,000 ship visits to U.S. ports each year. This, too, is a daunting management challenge.

To implement the *Maritime Transportation Security Act of 2002* in a timely and effective manner, Coast Guard must balance the resources devoted to the performance of homeland and non-homeland security missions; improve the performance of its homeland security missions;

---

[28] DHS-OIG, *ACE Release 4 Post-Deployment Problems*, OIG-07-54, June 2007.
[29] DHS-OIG, *Audit of Targeting Oceangoing Cargo Containers (Unclassified Summary)*, OIG-05-26, July 2005.
[30] DHS-OIG, *Audit of Targeting Oceangoing Cargo Containers (Unclassified Summary)*, OIG-07-09, November 2006.
[31] DHS-OIG, *Targeting Oceangoing Cargo Containers 2007(Unclassified Summary)*, OIG-07-72, August 2007.
[32] DHS-OIG, *Audit of CBP Export Control Activities (Unclassified Summary)*, OIG-07-76, September 2007.

maintain and re-capitalize Coast Guard's Deepwater fleet of aircraft, cutters, and small boats; restore the readiness of small boat stations to perform their search and rescue missions; and increase the number and quality of resource hours devoted to non-homeland security missions. For example, while overall resource hours devoted to Coast Guard's homeland security missions grew steadily from FY 2001 through FY 2004 and decreased marginally in FY 2005 and FY 2006. The Coast Guard continues to experience difficulty meeting its performance goals for homeland security missions.[33]

[33] DHS-OIG, *Annual Review of Mission Performance, United States Coast Guard (FY 2005)*, OIG-06-50, July 2006.

Management's Response to Major Management Challenges Facing the Department of Homeland Security

Management's Response to Major Management Challenges Facing the Department of Homeland Security

The Reports Consolidation Act of 2000 requires that the Department include a statement by the Inspector General that summarizes the most serious management and performance challenges facing the Department and briefly assesses the progress in addressing those challenges. The Office of Inspector General (OIG) considers the most serious management and performance challenges to the Department to be in the following areas:

- 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.

In addition to the OIG report on management challenges, in their biennial High-Risk Series, the Government Accountability Office (GAO) identifies federal programs and operations that are high-risk due to their greater vulnerabilities to fraud, waste, abuse and mismanagement. In recent years, GAO has also identified high-risk areas to focus on the need for broad-based transformations to address major economy, efficiency, or effectiveness challenges. Four of these areas fall within the Department's purview. The areas and the year the issue was identified are listed below. The GAO maintains these issues in their High-Risk Series until satisfied that acceptable progress has been made to correct the issues.

- Protecting the Federal Government's Information Systems and the Nation's Critical Infrastructures (1997);
- Implementing and Transforming the Department of Homeland Security (2003);
- Establishing Appropriate and Effective Information-Sharing Mechanisms to Improve Homeland Security (2005); and
- National Flood Insurance Program (2006).

The Department of Homeland Security has steadfastly worked to resolve the challenges identified in the Inspector General's FY 2007 report and the GAO High-Risk Series. The Department will continue to address the unresolved challenges, many of which may require several years to completely address due to the complexity of the challenge. The following highlights the accomplishments of the Department during FY 2007, and details some of the remaining plans to be completed to overcome these challenges.

FY 2007 Challenge 1: Catastrophic Disaster Response and Recovery

Summary of 2007 Challenge: OIG noted that the Department's failures after Hurricane Katrina illuminated a number of issues, including questionable leadership decisions and capabilities, organizational failures, overwhelmed response, communications systems, and inadequate statutory authorities. Coordination of disaster response efforts, catastrophic planning, logistics, acquisitions, housing, and evacuation were among the problem areas cited by the OIG.

2007 Accomplishments

- Operational planning is a core competency of the new FEMA. To strengthen our response capabilities, operational planners have been hired at FEMA headquarters to provide the ability to perform sophisticated operational analyses, analyze trends, and improve planning for the response to ongoing and future events. Planners are also being hired for the Regions to provide this same capability. With the new staff, there is now greater depth and capability to prepare operational plans and conduct crisis action planning to ensure that the agency can lead and support a national all-hazard emergency management response.
- Under a Gap Analysis Initiative rolled out by FEMA this past spring, a Gap Analysis tool was developed in coordination with the State of New York Emergency Management Office/New York City Office of Emergency Management, and implemented to provide FEMA and its partners at both the State and local levels in the hurricane prone regions of the country a snapshot of asset gaps. Seven critical areas were incorporated in the initial application of the Gap Analysis tool for review: debris removal, commodity distribution, evacuation, sheltering, interim housing, medical needs, and fuel capacity along evacuation routes. Gap Analysis discussions provided an opportunity for local jurisdictions to ask specific questions of Federal and State officials and identify issues of critical concern to help long-term preparedness activities. Although the initial use of this very successful concept was utilized for the 2007 hurricane season, this process will be expanded to cover all hazards and applied nationwide in FY 2008.
- FEMA has instituted a major Catastrophic Disaster Planning Initiative that will improve response capabilities and complement the National Response Plan/Framework (NRP/NRF), National Incident Management System (NIMS), and Federal, State, and local planning activities. This initiative addresses both notice and no-notice events, and reflects the considerable measures that DHS and FEMA and its Federal, State, and local partners have taken to ensure appropriate, quick, effective, and efficient response and recovery to protect the health, safety, and well-being of the population and, to the extent possible, restore the infrastructure following a catastrophic event. FEMA's Catastrophic Disaster Response Planning Initiatives are currently focused on four specific geographic areas: southeast Louisiana, the eight states in the New Madrid Seismic Zone (NMSZ), the State of Florida, and the State of California.
- A Mass Evacuation Incident Annex has been developed to describe in more detail evacuation functions and agency roles and responsibilities in mass evacuations. It provides guidelines for evacuating large numbers of people in incidents requiring a

coordinated Federal response through the NRP/NRF Emergency Support Functions, and describes how Federal resources are integrated into State, local, and tribal support. In addition to the Mass Evacuation Incident Annex, FEMA is also working on developing an Incident Supplement to the Annex that will provide specifics regarding how and by whom many of the responsibilities outlined in the Annex will be accomplished. Issues such as evacuee registration and companion animal sheltering will also be addressed.

- FEMA has also developed a new and robust Office of Acquisition Management. Staffing has dramatically increased, from 98 in 2006 to 221 at the present, an increase of 123 acquisition personnel positions. Approximately 90 percent of acquisition positions are filled. The Office has been reorganized into three core branches for greater efficiency of operations.
- Other acquisition accomplishments:
    - Developed a Disaster Response Training Course which is required for all acquisition personnel at HQ and in the Regions who will be deployed at a disaster.
    - Issued an Emergency Acquisition Field Guide to assist non-contracting personnel in effectively and appropriately contracting for goods and services in an emergency situation.
    - Established a Contracting Officer Technical Representative (COTR) Training Program.
    - Pre-positioned agreements have been established by determining what types of goods and services are traditionally utilized in a disaster. This ensures industry contracts are competitive and have a reasonable price and allows for a more responsive industry focus ensuring quick mobilization. Prior to Hurricane Katrina, there were nine contracts in place. There are currently 40 contracts pre-positioned for use in a disaster.

Remaining Plans

- FEMA plans to continue its aggressive staffing policies by filling vacant positions and maintaining high staffing levels and succession planning. Training will also be a key element. The Disaster Training Course and Emergency Acquisition Field Guide will be updated as necessary. All acquisition personnel will be given training and course changes and updates will be made via the Virtual Acquisition Office. COTR training will also be emphasized. FEMA will ensure that the COTR Training program remains current by hosting refresher courses as necessary and implementing a tiered COTR certification program in order to better match COTR competencies to contract complexity.
- FEMA plans to implement the DHS-standard (PRISM) contracting writing system which will provide FEMA's Office of Acquisition Management with
    - better workload tracking,
    - more consistent and accurate reporting,
    - improved contract writing and overall management, and
    - enhanced and more efficient use of other Federal acquisition personnel as approximately 64 percent of Federal agencies use this application.

- FEMA also plans to develop contract administration procedures for cost and schedule oversight for other national procurements.
- FEMA will develop and roll out the capability for long-term recovery planning at the operational Joint Field Office level.

FY 2007 Challenge 2: Acquisition Management

Summary of 2007 Challenge: OIG commented that DHS tends to focus its strategies on the urgency of meeting mission needs, rather than balancing urgency with good business practices, leaving the Department vulnerable to spending millions of dollars on unproductive investments. Common themes and risks include the dominant influence of expediency, poorly defined requirements, and inadequate oversight, which can contribute to ineffective or inefficient results and increased costs. Of specific concern is the USCG's Deepwater program and CBP's Secure Border Initiative Network (SBInet).

Office of the Chief Procurement Officer (OCPO)

2007 Accomplishments

Acquisition Policy & Legislation (APL)

- OCPO Acquisition Policy Board - OCPO stood up the OCPO Acquisition Policy Board. The Board's membership consists of each Component's Head of the Contracting Agency (HCA) Policy chiefs as well as a member of OCPO's Oversight staff. The purpose of the Board is both to disseminate Department-wide acquisition policy information, as well as foster dialog between Component staff members.
- Performance-Based Acquisition (PBA) - DHS OCPO has for much of the year been actively engaged in the Office of Federal Procurement Policy's (OFPP's) PBA Interagency Working Group. The Group has worked to enhance OFPP's PBA Seven Steps Guidance and make available appropriate samples tailored to Component needs. Additionally, OCPO Oversight has begun during its Component reviews to check acquisitions coded in the Federal Procurement Data System (FPDS) as performance-based to verify if the contracts are in-fact performance-based. PBA was also one of the very first Excellence in Contracting training topics.
- Federal Acquisition Regulation (FAR) Cases – Through its representation on the Civilian Agency Acquisition Council, OCPO is very engaged in all regulatory changes to the FAR. OCPO's active involvement ensures that the balance between good business decisions and urgency is a consideration when government-wide acquisition regulations are promulgated.
- Policy Guidance on Service Contracts – Because DHS utilizes a substantial amount of services contracting, the Chief Procurement Officer issued a memo to Components which reminded acquisition professionals of the range of types of services contracting and certain restrictions that apply to each.
- Source Selection Guide – During FY 2007, OCPO issued a Source Selection Guide that provides extensive guidance on conducting formal source selections under FAR Part 15

designed to improve effectiveness in the acquisition process without sacrificing efficiency.

- Improving Competition – OCPO held a Competition Advocates meeting to review DHS achievements and stress the importance of improving upon those achievements; established a Competition Award to recognize significant achievement in strengthening competition; issued an Acquisition Alert spearheading an initiative for Components to correct existing records; and began a systematic review of FedBizOpps sole source announcements to ensure that authorities are being appropriately used.
- Interagency Acquisition (IAA) – OCPO sees IAAs as an area of risk and therefore has been an active member of OFPP's Interagency Working Group crafting the first government-wide comprehensive guidance on IAA in accordance with the Services Acquisition Reform Act Panel's recommendations. OCPO is working to ensure that the final product meets our needs.
- Emergency Acquisition Flexibilities Guide – OCPO coordinated comments from Components on the draft OMB guide that was published in May 2007. Use of the Guide during emergency situations will enhance the Department's ability to complete acquisitions in a timely manner.
- Suspension & Debarment – OCPO participates on the Interagency Suspension and Debarment Committee (ISDC) established by Executive Order 12549. ISDC issues regulations with government-wide criteria for procurement and non-procurement programs, facilitates lead agency coordination, and serves as a forum to discuss current suspension. As a result of a July 18, 2007 Congressional hearing on responsibility issues, OCPO's Acquisition Policy and Legislation branch (APL) compiled an extensive list of Federal Government Business Systems, other public sector, nongovernmental or State/city systems or entities regarding business information that may be used as a source of information. APL is also participating in the discussion and analysis of an ongoing ISDC Information Sharing project in response to GAO's study (July 2005) on six Federal agencies which included management of "administrative agreements" and "compelling reasons determinations" to continue performance.

Acquisition Oversight

- DHS issued Management Directive 0784 formally initiating a DHS wide acquisition oversight program. Under this program DHS in partnership with Component leaders manage the DHS acquisition function. To date, the acquisition organizations have performed a self assessment and have begun to report key metrics on a quarterly basis. These metrics facilitate internal management and provide a verification mechanism to ensure that data available to external organizations is accurate and complete. Currently each of the acquisition organizations is undergoing a baseline review of the human resources capacity, adherence to policies and procedures, and status of IT systems to facilitate acquisitions and integration with financial systems. To date, OCPO has completed the baseline reviews of four Components and scheduled the remainder of reviews for FY 2008.
- Acquisition Oversight conducts special reviews of specific high-risk acquisitions assessing all aspects of the acquisition in support of DHS' mission and provides a risk analysis and recommends improvements for the instant acquisition. Where applicable the

review also recommends systemic changes, revised policies, or improved training to reduce risk for future acquisitions.

- With respect to improving the management of service contracts, DHS conducted training and additional oversight of service contracts to ensure compliance with Federal regulations and procured services were provided. OCPO has internal capability to monitor and investigate high-risk contracts to provide DHS with additional ability to manage and control.

Acquisition Systems

- Enterprise PRISM Instance (EPI) – DHS assumed control of the firewall, thereby strengthening the system security. Several on-going efforts to improve internal business processes and controls and increase the use of PRISM functionality are underway. Several examples follow. Because EPI is not presently interfaced to the accounting system, in partnership with the Finance and Program Offices, processes have been instituted to prevent inconsistent recording of contract obligations in the finance system. Workshops are being conducted to improve user efficiency and to identify areas for improvement. Reports are being utilized to ensure that PRISM transactions are accurate and complete. Training documentation has been customized to implement best practices and to marry policy with system functionality.
- Enterprise Acquisition System Initiative (EASI) - The consolidation effort of Component contract writing and management systems continues to make progress. In FY 2007 work began on the interface between EPI and FEMA's financial system.
- Federal Procurement Data System-Next Generation (FPDS-NG) - Verification and Validation Plan was developed along with additional HSAM policy to improve timeliness and accuracy of reported data. DHS representatives are participating in the FPDS-NG Change Control Board and User Group to continuously improve procurement reporting.
- Acquisition Systems Governance Board (ASGB) – This is a DHS-wide community of practice which meets on a regular basis to share leading practices and lessons learned on DHS Shared eAcquisition Systems. ASGB provides input to the Department in developing strategies for new automation products and services which support the acquisition function.

Strategic Sourcing Program

- In FY 2007, the DHS Strategic Sourcing Program (SSP) continued to leverage leading practices to optimize its program and ensure continued support for DHS' commodity councils and for Component specific business efforts. Positive results in price reductions, cost avoidances, and socioeconomic participation continued to be impressive, with the following delivered:

    - Cost Avoidance - Achieved $99,252,306 in Price Reductions and $690,714 in Cost Avoidances. These results were achieved by multiple initiatives across eight of DHS' 14 commodity councils;
    - Deliveries - Delivered eight distinct strategically sourced vehicles that will potentially place billions of dollars with small business while meeting the stringent operational requirements of DHS' end-users; and

- Performance Measures - Implemented various performance measures, in addition to price reductions and cost avoidances, to gauge the success of its programs. Representative performance measures that were utilized during FY 2007 included reduced downtime, total costs for maintenance moves and installation reductions, and awards, recognition, and customer satisfaction surveys.

Program Management

- OCPO has reorganized to include a Program Management SES-level directorate to develop and disseminate policy on program management to DHS Components.
- Additional certified program managers (PM) are now on board as a result of various DHS PM training programs, totaling 237 certified program managers since December 2006. This is a 53 percent increase in the past nine months.
- Additionally, in September 2007, a Memorandum of Agreement (MOA) was signed between the DoD and DHS. This strategic relationship enables DHS to take direct advantage of the Defense Acquisition University's acquisition, technology and logistics expertise in training, consulting, knowledge sharing, continuous learning, career workforce planning, and management services.
- One of the Chief Procurement Officer's top priorities is to build a strong acquisition system, with the right people, in DHS. OCPO is doing that through initiatives such as building standards for all acquisition professionals in DHS, installing a metrics system to measure cost, schedule and performance of major programs, and redesigning the investment review process, as examples. OCPO is also hiring experts in various acquisition career fields to build those competencies and systems throughout DHS. OCPO already has several program managers, cost estimators, Testing & Evaluation personnel, and a logistician at present.
- OCPO initiated program reviews on designated Level 1 investments, to strengthen the investment review process and provide greater independent analysis in an effort to mitigate risk. These reviews are scheduled for completion in first quarter FY 2008, with more extensive reviews as needed. This initiative is a three-prong approach in helping to identify and mitigate high-risk areas, provide a mechanism for sharing best practices, and promulgate policies and processes, as well as identify competencies gaps/training needs.
- Additionally, OCPO uses the Program Management Council, co-chaired by an operational program manager and the CPO, as a Department-wide forum for involvement as DHS builds acquisition expertise.

Acquisition Workforce

- Established framework for a developmental program to bring in up to 60 entry level positions in the 1102 career field, train the interns and provide broad experience across DHS to assist in closing the gap in contracting career field vacancies.
- Improved certification process for the three current acquisition career fields within DHS Program Managers, Contracting Officer Technical Representatives, and Contract Specialists.
- Participated in Government-wide emergency contracting working group to identify a cadre of specially trained contracting officers to provide support in catastrophic emergencies.

- Established and managed training for the 1102 career field within DHS. Conducted one hour DHS wide training sessions to address specific acquisition issues and immediately address gaps in training or acquisition processes.

Office of Small and Disadvantaged Business Utilization

- Met OCPO's goal of making good business deals and supporting public policy objectives such as the Federal small business program. The U.S. Small Business Administration recently recognized DHS in their first annual small business scorecard with a score of green, one of only seven out of 24 Federal departments to receive a green score.

Remaining Plans

Acquisition Policy & Legislation

- Emergency Procurement Tool Box/Framework – OCPO is currently working an initiative with FEMA to develop a framework in order to be able to expedite the acquisition function in the event of a significant national emergency, per the National Response Plan.
- Kaizen Event on Interagency Contracting - In conjunction with active participation in OFPP's Working Group developing a Government-wide Guide on Interagency Acquisition, OCPO is sponsoring and leading a Lean Six Sigma Kaizen event for the purpose of developing a Management Directive on Interagency Acquisition for the Department.
- Price Fighters Memorandum of Understanding (MOU) – OCPO is negotiating an MOU with Navy Inventory Control Point (NAVICP) to provide cost and pricing support for major Department acquisitions.
- Updating HSAM and/or Management Directive Guidance – seven documents are being developed.
- Electronic HSAR/HSAM - OCPO Acquisition Policy is engaged in integrating the HSAR and HSAM into a single electronic document to assist Component operational personnel with research Department acquisition policy. Future plans include providing links within the body of the revised HSAR/HSAM document to other applicable documents (e.g., memos, directives, training slides, etc.) to enable "one-stop shopping."
- Homeland Security Acquisition Regulation (HSAR) Cases – OCPO is engaged in developing seven DHS-only acquisition regulations.
- E-Verify – Crafted a Federal Acquisition Regulation rule to require Federal contractors to verify the employment eligibility of their employees. OMB approved going forward. The FAR change is currently in process. This is a major step in increased enforcement of ensuring only eligible persons work in the United States.
- Time and Material (T&M) Contracts – OCPO is developing guidance on the use of T&M in response to recent changes in Government-wide T&M policy.
- Competition – Various activities for improving the level of competition are currently in process.
- Contract Funding Guidance – Guidance on contract funding is currently in review. It discusses FAR contract funding policies and clauses to assist Contracting Officers in developing effective strategies that afford the maximum benefit to DHS contracts and programs.

- Blended Workforce Initiative- Discussions are underway regarding the development of a reporting system to obtain information from contractors on the types and amounts of contracted labor being performed under DHS' services contracts for the purpose of enabling DHS to better manage use of contractors performing functions on behalf of DHS.
- Acquisition Guidelines – APL plans to develop new form of communicating with Components to provide timely "how to" and interpretive guidance. This will be a series of "Acquisition Guidelines" that will be published on the web and will be linked to and from various HSAR/HSAM policies.

Acquisition Oversight

- Of the eight full acquisition organizations, four baseline onsite acquisition reviews are physically complete. The remaining four have been scheduled and will be completed by October 2008.
- Review of the full role of acquisition oversight.

Acquisition Systems

- EPI Rehost - EPI will be moved to the DHS Hosting Facility in FY 2008. This is to increase system security.
- Enterprise Reporting – will improve reporting and management controls by increasing data sharing which will enable better business decisions.
- EASI - FEMA and FLETC are scheduled to go live on EPI.
- eInvocing – will reduce Prompt Payment Act interest penalties and streamline the invoice approval process.

Program Management

- DHS currently has three acquisition career fields for which DHS has certification standards (Contracting Officer, Contracting Officer's Technical Representative, and Program Manager). DHS will be adding certification standards for other acquisition career fields, including logistics, systems engineering, cost estimating, and test and evaluation as soon as practicable. OCPO plans to meet both the civilian agency standards, where they exist (currently for contracting and program management), as well as meeting the DAWIA standards, so as to ensure the Department has the best acquisition workforce.

- DHS is retooling the process for reviewing and approving major Department programs and has begun its review of existing programs to determine how to proceed.
- OCPO is conducting Quick Look reviews of all Level 1 acquisition programs. The Quick Look Reviews are designed to provide a rapid assessment of the risk in the Level 1 Acquisition Program Portfolio. The results will be used to identify any high-risk programs for which a more in-depth review may be tasked. These reviews will also provide insight into Component governance and oversight processes that DHS can leverage to refine Departmental acquisition policies and processes.

Acquisition Workforce

- FY 2008 will be the first fiscal year implementing the new intern training and development program. As implementation proceeds, additional interns will be added and improvements to the program will be instituted.
- Additional acquisition career fields required for successful execution of acquisition programs will be identified. Specific training and certification requirements will be assessed for each of these new career fields.
- A mechanism to identify acquisition corps members will be developed.
- Training funds will be centralized to efficiently ensure that all acquisition corps members receive prompt training so they can better perform the mission and improve within the career field.
- Recruitment efforts will be centralized to improve efficiency.

U.S. Coast Guard Deepwater Acquisition

Five years into this 25-year acquisition, USCG has overcome many significant challenges, though more remains to be done. As a result of those lessons learned, USCG is taking aggressive action to strengthen program management and execution. By redefining roles and responsibilities, fundamentally changing relationships with industry, and by strengthening the assessment of government and industry performance, the Deepwater program is showing notable improvements in multiple areas.

2007 Accomplishments

Stand-up of the Acquisition Directorate

- As outlined in the Blueprint for Acquisition Reform, one important objective was to establish a consolidated acquisition directorate which initially came together on July 13, 2007. As part of this consolidation, the Acquisition Directorate, the Deepwater Program Office, the Office of Procurement Management, the Office of Research, Development, and Technical Management, the Research and Development Center, and the Head of the Contracting Authority have been brought together under one roof, led by an Assistant Commandant for Acquisition. This means that USCG is better able to allocate its contracting and acquisition professionals and resources to focus on excellence in program management and contract execution. This is expected to create more efficient and consistent processes, leading ultimately to a more effective acquisition organization.

Changes in the Contract Structure

- As the OIG has suggested, USCG agrees that working closely with industry is still the best approach to recapitalizing and modernizing USCG's platforms and mission systems. However this relationship must be based on sound business practices to ensure suppliers can meet the Government's requirements while adhering to cost, schedule and performance parameters. Therefore, in all dealings with the private sector, USCG is ensuring new acquisition contracts are clearly written and provide for careful Government oversight and management of manufacturer's cost, schedule, and performance.

- In an effort to better define program requirements, USCG has improved the detailed Delivery Task Orders by increasing the use of Statements of Work specifications as compared to Statements of Objective. This reflects a strategic change for USCG by transitioning from a pure performance based approach for assets towards more explicit contract language which includes relevant specifications, standards, and increased written detail as recommended by OIG.

Implementing the Blueprint for Acquisition Reform

- To guide its acquisition reform and business transformation initiatives, USCG developed and published its own strategic and overarching vision called the Blueprint for Acquisition Reform modeled after that developed by GAO for the assessment of Federal Government acquisition processes.
- The success or failure of USCG's acquisition reform initiatives will be tracked by two tiers of metrics. The first is to measure activity called for in the Blueprint on how USCG is doing in executing the plan of action and milestones that are outlined in the Blueprint.
- A more important metric, which will be longer in coming, is the measurement of return on investment measured against project cost, schedule, and performance. It will take time to generate that strategic assessment, "How does the Blueprint reflect back on Coast Guard project and program execution?"

Establishing a Capable Acquisition Workforce

- USCG has built a much more capable acquisition organization than it has ever had. Among many attributes this right-sized dedicated USCG acquisition workforce incorporates two underlying principles: (1) reinvigorated and documented use of a technical authority, outside the acquisition directorate, for all major projects and (2) partnering with other government agencies whenever additional competencies are needed.
- Some of the significant accomplishments during 2007 were:
    - Creating a standard Project Management Core Team model, which is consistent across all USCG acquisition projects and includes all critical functions in support of project execution;
    - Conducting an assessment of current certification levels to ensure personnel are aligned with their respective roles and expected outputs; and
    - Evaluating, and revising as necessary, position descriptions for proposed new hires.

Improvement of Technical/Program Oversight

- The Assistant Commandant for Engineering and Logistics has been designated as the technical authority for all designs and design changes, the Assistant Commandant for Operations for definition of asset performance requirements, and the Assistant Commandant for Command, Control, Communications, Computers, and Information Technology (C4IT) as the technical authority for all Command, Control, Communications, Computers, Intelligence, and Reconnaissance (C4ISR) systems and equipment. Additionally, the Assistant Commandant for Human Resources is the technical authority for all USCG human resource issues. This means that project and

program managers, as well as associated contracting and acquisition professionals, have a direct link back to technical and operational experts to ensure that designs are technically robust, meet standards and are supportable.

- In order to strengthen Government management and oversight of the Deepwater program, as well as to better position USCG to fully oversee the contractor and effectively adjudicate technical concerns, all Integrated Product Teams (IPT) must be chaired by a USCG officer or employee. That change was executed in March 2007. Additionally, all IPT charters have been re-examined to determine where other changes are needed. USCG leadership of IPTs means USCG is better able to resolve non-major technical concerns or, where concerns persist, raise them to the appropriate management and contracting levels for adjudication.
- To ensure that designs and assets will meet USCG needs, there has been in increase in the use of independent, third-party review and analysis (in concert with the USCG technical authorities) for all new starts or substantial design changes. Inherent in this initiative is a renewed commitment to utilize full business case analyses for all new acquisition decisions to instill confidence that USCG is building and buying the right tools for our Coast Guard men and women and at the best value for taxpayers.
- The Directorate has placed renewed emphasis on the USCG's Major Systems Acquisition Manual (MSAM) and DHS-sanctioned processes for program management and acquisition.

Remaining Plans

Alternatives Analysis

- USCG's Acquisition Directorate has asserted its role as the lead systems integrator across its entire $27 billion investment portfolio. The investment portfolio includes the 25-year, $24 billion Integrated Deepwater System (IDS), the largest of eight major acquisition programs. The IDS program modernizes and recapitalizes legacy surface, air, and shore assets to enable USCG to deploy more capable and interoperable offshore maritime patrol and interdiction forces. As lead systems integrator, USCG has restructured Deepwater and the rest of the Coast Guard's acquisition investment portfolio under the aegis of proven acquisition policies and processes, including the procurement principles outlined in USCG's MSAM.
- MSAM requirements state that an Alternatives Analysis (AA) should be conducted and updated whenever significant changes occur in requirements, life cycle cost estimates, or return on investment assessments. The original Deepwater AA was conducted by industry teams as part of the Deepwater proposal process (circa 2001). Operational requirements and design changes that have evolved since September 11, 2001 make it prudent and timely to conduct an independent AA at this time, in order to ensure that USCG continues to acquire systems that fully meet its mission needs. Therefore, in accordance with requirements set forth in the MSAM, the Coast Guard is conducting a state-of-the-market AA of the Deepwater program. The AA will be a program-wide analysis and will include an assessment of the major systems and platforms within the IDS projects. The AA is a positive step in that it aligns with best practices established through DHS and OMB acquisition policy.

Workforce Management Analysis

- The USCG Human Capital Strategy will include a Long-Range Workforce Plan for the entire USCG Acquisition Directorate. The Long-range Workforce Plan will describe the specifics of the necessary workforce over several years. It will forecast and convey the specific skill sets and competencies needed, broken down by both full time equivalent and functional area. The Long-range Workforce Plan will be a dynamic plan linked to acquisition program execution schedules, maintained by Acquisition Program and Project Managers. This dynamic linkage will allow human capital managers to plan for future workforce needs well in advance, and to react swiftly to changes in acquisition strategy initiated at the program or project level.

SBI*net* Management

2007 Accomplishments

Fielding Border Surveillance Technologies/SBInet Program Management

- CBP awarded an SBI*net* task order to demonstrate the effectiveness of the overall approach to SBI*net* along 28 miles of border flanking the Sasabe Port of Entry in Arizona. CBP has made significant progress in implementing Project 28, including deploying all nine re-locatable camera and radar towers, and fitting all 50 of the Project 28 agent vehicles with Common Operating Picture hardware.
- Under the SBI*net* prime contract, CBP awarded a task order for the test and evaluation of fencing solutions. The purpose was to test effective low-cost solutions that meet operational requirements and can be reproduced for rapid deployment along the Southwest Border. This testing will help CBP add to existing tactical infrastructure to reach a total of 370 miles of fencing and 200 miles of vehicle barriers by the end of calendar year 2008.
- CBP met its commitment to construct 70 miles of primary fencing along the Southwest Border. This effort was comprised of both new and previously planned projects brought together under SBI*net*.
- CBP formed a Secure Border Initiative (SBI) Executive Steering Committee (ESC) to provide oversight of the implementation of SBI and SBI*net*. The SBI ESC serves as an advisory board, helping the SBI Executive Director to effectively implement program management decisions.
- SBI is developing, documenting, and implementing sound program and performance management processes. SBI developed a process asset library, with a baseline of 76 program management policies, plans, processes and procedures. The program has established scheduling standards for the development and maintenance of the Integrated Master Schedule and project schedules. SBI has established processes and procedures for Earned Value Management System baseline analysis and reporting. Monthly Program Management Reviews, which address cost, schedule, performance, and risk – are conducted to monitor the program progress. Oversight of Prime contractor deliverables are performed to ensure measures and metrics reported are consistent and traceable to the Quality Assurance Surveillance Plan.

- SBI and SBI*net* have significantly increased organizational capacity, adding 168 staff members to help manage the program and address crosscutting issues such as coordination with USCG on maritime border security issues.

Remaining Plans

Fielding Border Surveillance Technologies / SBInet Program Management

- CBP is committed to build a total of 370 miles of fence and 200 miles of vehicle barriers along the Southwest Border by the end of calendar year 2008.
- CBP is committed to deploying 70 communications, camera, and radar towers by the end of calendar year 2008.

FY 2007 Challenge 3: Grants Management

Summary of 2007 Challenge: The OIG letter acknowledges that managing the multitude of grant programs within DHS poses a significant challenge. Further, the grant programs of other Federal agencies that assist State 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 with similar, if not identical, purposes. However, they comment that the Department must do more to coordinate and manage grants that are stove-piped for specific, but often related purposes, to ensure they are contributing to our highest national preparedness and disaster recovery goals, rather than duplicating one another and being wasted on low-priority capabilities.

2007 Accomplishments

- FEMA streamlined business processes from three legacy organizations into one FEMA Grants Directorate (transitioned legacy Preparedness Grants into FEMA).
- FEMA migrated the Grants and Training IFMIS Financial System and the Payment and Reporting System web system from the Office of Justice Programs to FEMA.
- FEMA stood up a Grant Programs Directorate with no additional resources and awarded over $4 billion dollars in non-disaster Federal assistance while working through transition issues of migrating the Office of Grants and Training to FEMA.
- FEMA provided advanced level grants management training to States, local governments, non-profit organizations, and other grantee recipients all across the country and in the territories.
- FEMA Headquarters (HQ) collaborated with its Regions to interview 20 Grants Management Specialists (GMS) to begin financial grants work related to transitioned preparedness grants in the Regions. This was a huge undertaking for both HQ and Regional offices as these positions came as a result of the reprogramming and were announced and interviewed in a short timeframe.

Remaining Plans

- FEMA is striving for strong collaboration with its Regional offices to work towards the new FEMA vision.
- FEMA will hire and train 20 new Grants Management Specialists in the Regions to facilitate more coordination with local partnerships.
- FEMA is working to transition the administration of preparedness grants to FEMA Regional offices.
- DHS is in the process of streamlining all the DHS grant management business processes to provide oversight monitoring capability as well as unified grant management processing.
- DHS HQ is establishing a DHS-wide audit tracking system that will record and track resolution completion for the A-133 audit process. This will ensure that audits are resolved in a timely manner and that trends in audit findings are addressed.
- DHS is working with the OIG in reviewing the 36 Federal assistance programs (identified as potential programs that may duplicate DHS programs) to determine if they duplicate or complement DHS programs.
- DHS HQ is anticipating the transfer the Office of Grant Policy and Oversight from the Office of the Chief Procurement Officer to the Office of the Chief Financial Officer in order to provide resources for a more robust oversight capability related to accountability of funds, internal controls and audit processing.

FY 2007 Challenge 4: Financial Management

Summary of 2007 Challenge: Per OIG, financial management is a significant challenge for DHS. A number of material weaknesses in internal control continue to exist. The material weaknesses in internal control are impediments to obtaining an unqualified opinion and have precluded management from giving positive assurance over internal control at the Department level. DHS' ability to obtain an unqualified audit report, and provide assurances that its system of internal control is designed and operating effectively, is highly dependent upon process and procedural improvements across DHS.

However, the Department notes that many of our material weaknesses were inherited and are longstanding challenges. These challenges will not be solved in a single step, but through near and long-term fixes. The auditor's reports highlight the challenges we face. They identified weaknesses that have occurred for a variety of reasons common to newly formed organizations, such as inconsistent processes, reliance on legacy policies, undeveloped internal controls, incomplete and inaccurate information, or systems that cannot properly process reliable data and information. But we are not stopping at simply fixing what the auditors find. One of the most important lessons learned from our initial years of implementing the DHS Financial Accountability Act involved shifting from just focusing on audit opinions or addressing auditor-identified issues to also building support for the Secretary's Assurance Statement by focusing on management-identified root causes and management-performed test work. While audit outcomes are important, we will also concentrate on management's responsibility for internal controls. Through our multi-year internal controls assessments, we are documenting the design

of our controls to best discover the root causes of a problem and to guide our corrective action efforts. We will then test their operating effectiveness to build support for the Secretary's Assurance Statement.

2007 Accomplishments

- On March 1, 2007, the Secretary and Chief Financial Officer issued the inaugural version of the Internal Control Over Financial Reporting (ICOFR) Playbook. The ICOFR Playbook represents an ambitious multi-year effort to build assurances and retire material weakness conditions. Highlights of significant FY 2007 accomplishments include:
  - Strengthened the control environment within the Office of the Chief Financial Officer and bolstered financial management and oversight functions with the strong support of the Department's Secretary and Under Secretary for Management;
  - Implemented Department-wide financial reporting process improvements;
  - Developed Department-wide financial management policies and procedures;
  - Developed standard operating procedures at TSA to improve financial reporting control activities;
  - Provided oversight and held Component management accountable for financial system security corrective actions through partnership between the Under Secretary for Management, Chief Financial Officer, Chief Information Officer, and Chief Information Security Officer, resulting in compliance with the Federal Information Security Management Act;
  - Implemented policies and procedures to improve accounting for legal contingent liabilities, intragovernmental and interdepartmental reconciliations, and capitalization of internal use software; and
  - Sustained FY 2006 progress at ICE and eliminated all remaining ICE material weakness conditions.

Remaining Plans

- Significant challenges remain at USCG and FEMA. To support these Components, the Department's Chief Financial Officer conducts monthly corrective action meetings with Senior Management and weekly working group meetings with Senior Staff. Highlights of these support efforts include:
  - Setting USCG priorities for resolution of ten material weakness conditions, based on risk, resource availability, mission impact, and other factors.
  - Partnering with the Under Secretary for Management and Department's Chief Procurement Officer to strengthen management and oversight functions at FEMA and establishing internal controls for delivering benefits and assistance to disaster victims.
- A summary of planned corrective action efforts is provided within the Other Additional Information's Summary of Financial Statement Audit and Management Assurances section.

FY 2007 Challenge 5: Information Technology Management

Summary of 2007 Challenge: According to OIG, integrating information technology (IT) systems, networks, and capabilities of the various legacy agencies to form a single infrastructure for secure, effective communications and information exchange remains one of DHS' biggest challenges. OIG believes it is essential that DHS implement a Department-wide program to ensure effective information security controls and address IT risks and vulnerabilities. They also believe it is critical that the Department acquire and implement systems and other technologies to streamline operations within DHS Component organizations, and to support effective information sharing with State and local governments, the private sector, and the public. Finally, they opine that DHS is challenged in addressing privacy concerns while integrating its myriad systems and infrastructures.

Department-wide IT Infrastructure

2007 Accomplishments

Department-wide IT

- Completed 50 percent of IT projects within 10 percent of the cost and schedule dates.
- Integrated information security architecture with DHS Enterprise Architecture (EA), System Development Life Cycle (SDLC), Capital Planning Investment Control (CPIC), and acquisition processes.
- Implemented National Institute of Standards and Technology (NIST) SP 800-53 in policy and information security compliance tools.
- Developed and deployed the DHS Information Security Scorecard for communicating departmental progress in Certification and Accreditation (C&A), FISMA Compliance and Weakness Remediation.
- Consolidated IT support for unclassified, Secret, and Top Secret local area networks (LANs) into a single vendor to improve service delivery and cost efficiency.
- Leveraged delivery of infrastructure operations and management (O&M) to capture additional cost reductions and efficiencies as the population continues to grow.
- Supported the migration of legacy data centers to two DHS Data Centers.
- Increased the use of IT research and advisory service contracts by DHS personnel by 100 percent over the prior year.
- Developed and initiated a plan to establish test facilities at the DHS enterprise data center.
- Developed a plan to integrate DHS IT test facilities and consolidate these with data centers in coordination with Science and Technology Directorate.

Information Technology Services

- Continued the enterprise implementation of the Department-wide Smart Buy enterprise license agreement for access to Geographic Information System (GIS)

software/training, saving DHS approximately $4 million over General Services Administration (GSA) list pricing.

- Coordinated a Department-wide investment in geospatial data through partnership with the National Geospatial-Intelligence Agency and the U.S. Geological Survey, achieving $12 million in cost avoidance.
- Implemented the Enterprise Information Repository to support IT security, portfolio management, program oversight, and Enterprise Architecture governance.
- Completed the target architecture for the Technology Reference Model (TRM), including completion of Enterprise Architecture (EA) TRM insertion packages for 18 critical technology areas.
- Formalized a strategy for the enhancement of information sharing by developing and enhancing workflow, document management, and Business Process Management (BPM) capabilities to increase user satisfaction by 40 percent and decrease cost by 15 percent while also reducing production time by 25 percent.
- Established a repeatable process for the DHS CIO to approve procurements that contain IT elements of $2.5 million and above to ensure that all contracts fully comply with FISMA;
    - Partnered with the Office of Procurement Operations (OPO) and Chief of Administrative Services (CAO) to share data to provide offices with advanced notice of procurements and purchases of property.
    - Established preliminary performance measures that will be refined after at least 12 months of data are reported.
- Developed and executed the IT Budget Review Process, ensuring that IT requirements are integrated with the FY 2009-2013 Resource Allocation Plan data call. Reviewed and made recommendations regarding Component portfolio and investment IT budgets. Reduced duplication and showed cost savings of 5 percent of the budget of one portfolio through the analysis and implementation of recommendations.
- Complied with the President's Management Agenda (PMA) and the OMB mandate to implement and monitor Earned Value Management (EVM) and Operational Analysis (OA).
- Identified Portfolio Managers for all of the DHS Portfolios and half of the Portfolio managers directly contributed Portfolio analysis to the budget, acquisition, and investment review process.
- Implemented Application Authentication for: the Secretary's Priority Tracker, the Homeland Secure Information Network (HSIN), DHS' primary authentication service enabling E-authentication, and for the FedBridge capability for the Department. Identified and consolidated the Disaster Management (DM) technology platform onto the target HSIN platform, resulting in more than $2 million savings in FY 2007.
- Integrated Disasterhelp.gov with E-authentication, meeting the OMB milestones.
- Implemented new enterprise Learning Management Systems for DHS headquarters and several Components.
- Issued first DHS Smartcard in advance of the October 27, 2006 deadline.

Wireless Activities/Security Activities

- Processed 3,795 frequency assignment records in support of DHS operations including coordination of 410 assignment proposals and spectrum support for CBP Project-25 upgrade and modernization efforts in Arizona.
- Jointly led with the Department of Justice (DOJ) government-industry interchange, design competition, and final selection for $10 billion, 15-year Integrated Wireless Network contract vehicle.
- Established a primary Network Operation Center (NOC) and Security Operation Center (SOC) to full operating capability.
- Completed 90 percent of Component migrations to MS Exchange.

Homeland Secure Data Network

- Established a second backup data center at the Stennis, Mississippi data center to provide increased system availability and disaster recovery with 24/7 operations during times of national incidents or disasters.
- Established a secondary access point to DOD Secret Internet Protocol Router Network (SIPRNet) to increase availability to HSDN critical customers.
- Migrated the HSDN Backbone to OneNet, providing OneNet connectivity to the HSDN Data Center to support field site deployments on OneNet.

Information Security

- Comprehensive Certification and Accreditation process in place.
  - At the end of July 2007, 88 percent of FISMA systems had valid Authority to Operate letters.
- Improved Plan of Action and Milestones (POA&M) tracking process for remediating security weaknesses
  - Closed 363 of 438 IT security audit findings.
- Annual user IT Security Awareness Training is at or near 100 percent for all employees and contractors with system access.
- Configuration guides have been published for all operating systems in the department.
  - The Department has validated configuration compliance programs for all Components.
  - Components have reported that over 90 percent of systems in the Department have implemented configuration guides.
  - Percentage of systems that have completed annual National Institute of Standards and Technology Special Publication 800-53 assessments is over 90 percent..
- Enhanced security operations capability.
  - All Components now regularly report IT security incidents to the DHS Security Operations Center, who in turn report to US-CERT, as appropriate.
  - Improved DHS Security Operations Concept of Operations published in 2007, detailing specific enterprise-wide security operations procedures.

Remaining Plans:

Department-wide IT

- Maintain full FISMA compliance for each of 700+ systems in the Department's inventory.
- Complete the implementation of the plan to retire all financial systems security weaknesses.
- Update Security Policy and Architecture Guidance to address new operational requirements, advancing technology, and new threats as well as adapting new best practices.
- Complete a rigorous review and analysis of the standards, products, and services contained in the Technical Reference Model to ensure they comply with the Security Architecture.
- Begin to replace all IT hardware assets per National Capital Area (NCA) - developed replacement periods (e.g., wireless devices – 18 to 24 months, personal equipment – 36 months, and server/network equipment – 48 to 60 months).
- Conduct requirements gathering and planning for the development of the new consolidated DHS location at the St. Elisabeth's campus.
- Ensure capability readiness and migrate legacy data center systems to the two DHS Data Centers.
- Implement testing of information technologies at the DHS enterprise data center.

Information Technology Services

- Migrate 100 percent of DHS enterprise to Environmental Systems Research Institute (ESRI) SmartBuy investment.
- Stand up initial geospatial data warehouse capability at the DHS Enterprise Architecture and DHS' National Center for Critical Information Processing and Storage (NCCIPS) Data Center at Stennis, Mississippi.
- Deploy standardized and interoperable common operating picture (COP) technology, support the NOC, the National Infrastructure Coordination Center (NICC), and the National Response Coordination Center (NRCC), and formalize this architecture as part of the DHS Enterprise Architecture through the technology insertion process.
- Oversee the Single Sign-On integration with the DHS Portal Environment.
- 100 percent of IT Portfolios Managers will directly contribute Portfolio analysis to the budget, acquisition, and investment review process.
- 100 percent of DHS Portfolios will identify IT EA targets
- Initiate Portfolio Management framework across 25 percent of DHS Components.
- Complete the migration of consolidated Disaster Management technology platform onto the target HSIN platform.
- Continue implementation of the new enterprise Core Personnel system (EmpowHR) for ICE, USCIS and other Components.
- Implement new enterprise Learning Management Systems additional Components.
- Continue to implement new enterprise Recruitment suite of systems (ICE, USCIS, CBP, and other Components).

- Provide Program Management Support for Information Quality and ensure that the Department remains compliant.
- Provide Program Management Support for Government Paperwork Elimination Act and ensure that the Department remains compliant.
- Define standard capability for Smartcard issuance and scale for use by all Components.

Security Activities

- Move all remaining Components to OneNet with centrally managed Network Services with enterprise-wide NOC/SOC services.
- Establish a secondary NOC/SOC.
- Complete Component migrations to MS Exchange.
- Establish disaster recovery capability between the two DHS Data Centers.

Homeland Secure Data Network

- Establish and maintain periodic HSDN program self-assessment and evaluation through the DHS established Operational Analysis periodic review and reporting process in order to identify areas for improvements in costs and operational efficiencies and effectiveness.
- Establish support for the mission requirements of DHS Component organizations and homeland security partners staying abreast of and identifying applicable advancing information and applied technologies capable of improving data gathering, fusion, analysis, intelligence gathering and dissemination at a SECRET-classified level.

Information Security

- Comprehensive Certification and Accreditation process in place.
  - Goal is 100 percent of FISMA systems have valid Authority to Operate letters.
- Close all IT audit findings.
- Annual user IT Security Awareness Training is at 100 percent for all employees and contractors with system access.
- Configuration guides have been published for all operating systems in the department
  - The Department validates configuration compliance programs for all Components.
  - Percentage of systems that have completed annual National Institute of Standards and Technology Special Publication 800-53 assessments is 100 percent.
- Enhance security operations capability by continuing to report all IT security incidents to the DHS Security Operations Center, who in turn reports to US-CERT, as appropriate.

Component IT Management

2007 FEMA Accomplishments

- Started modernization and upgrade efforts to improve information sharing and functionality among six critical systems.
  - National Emergency Management Information System (NEMIS);

  - Logistics Information Management System (LIMS-III);
  - Automated Deployment Database (ADD);
  - Total Asset Visibility (TAV);
  - Integrated Financial Management Information System (IFMIS); and
  - Acquisition Management System (PRISM).
- Migrated the Grants and Training IFMIS Financial System and the Payment and Reporting System web system from the Office of Justice Programs to FEMA.
- Participated in two field operation demonstrations and exercises to test our interoperability with Federal, State and local response efforts, and our communications plans in order to identify failures or shortcomings, corrected by June 1, 2007.
- Expanded State and local communications planning efforts to include assistance in the development of interoperable communications plans for all States in Regions 4 and 6, Puerto Rico and the Virgin Islands, as well as all Emergency Support Functions that are on the Federal response team to assist in disasters.
- Acquired 34,000 licenses of the Asset Tracking Software (CompuTrace Complete) and deployed 3,399 licenses on laptops supporting disasters.
- Acquired 36,450 licenses for Full Disk Encryption software to support laptops used in support of disaster operations.
- Acquired 4,000 licenses of 2-Factor authentication solution as a FEMA pilot to comply with OMB M06-16.
- Replaced Egress and DMZ Firewalls that were becoming obsolete.
- Completed pilot on deploying an Enterprise Patch Management solution and developed schedule for Agency-wide deployment.
- Acquired software for Enterprise Patch Management solution and currently deploying agents.
- Installed NetIQ Security Manager on critical servers to monitor critical network devices, specifically egress firewalls, virtual private network concentrators and some ingress firewalls.
- Provided training for 28 Information Systems Security Officers.
- Completed plan to support and guide critical IT improvements with the following five Strategic Imperatives: 1) Stabilize and Integrate IT Assets Across the Agency; 2) Secure the IT environment; 3) Network the Agency; 4) Evolve to a "Service-Forward" Organization; and 5) Establish the Supporting IT Policy and Governance Structure.
- Continued refining and documenting IT management practices, policies, and procedures.
- Implementing Enterprise Architecture based standards of interoperability, security, and cost efficiency.
- Completed initial architecture-based analysis of systems.
- Identified mission critical systems.
- Determined mission needs through customer analysis and began work to identify functions that the Office of the CIO is currently capable of providing to meet needs.
- Began process of aligning system functions to meet FEMA's mission needs.
- Created system guidance to direct technical improvements and system upgrades.
- Upgraded several systems to improve their capabilities and ability to share information.
- Continued the monthly project management and professional development training sessions.

- Continued analysis of the optimal project and portfolio management tools and implementation options.

FEMA Remaining Plans

- Continue upgrade of six critical systems, NEMIS, LIM-III, ADD, TAV, IFMIS, and PRISM.
- Complete Mitigation Advisors Statistical Tracker.
- Improve operations and testing by creating Integrated Test Facility for software, updating the Test Development Laboratory servers, and evolving two testing environments to the required five environments which will allow NEMIS modules to be reengineered and replaced completely with a minimum number of disruptions (phased completion).
- Replace legacy servers to improve processing speeds, increase capacity, and reduce the number of replication cycles in the current systems.
- Deploy Emergency Management Mission Integrated Environment and migrate data to that system from Regional server.
- Deploy Document Management and Records Tracking System for multiple FEMA applications.
- Complete development of numerous Individual Assistance support systems including the National Shelter System, Fulsome letters, Web indexing code, Web Registration Intake, and the IA Center.
- Work with Emergency Management Institute to develop concurrent training plans and materials
- Acquire and deploy 10,000 additional licenses for Asset Tracking Software (CompuTrace Complete) on all FEMA laptops.
- Deploy Full Disk Encryption software to support 36,450 remote access users as a FEMA pilot Install 4,000 licenses of 2-Factor authentication solution (RSA) as a FEMA pilot to comply with OMB M06-16 Fully deploy Enterprise Patch Management Solution Agency-wide.
- Expand implementation of NetIQ Security Manager for any security-related events including failed logon attempts and configuration changes.
- Conduct security assessment to determine effectiveness of security measures to ensure secure sharing of information.
- Deploy Community Information System (CIS) v4.5 Code into production.
- Complete development of Electronic Fingerprint System (EFS).
- Complete Enterprise Oracle database improvements.
- Develop Emergency Management Information Management System (EMIMS).
- Complete Executive Management System v1.0 (EMS).
- Complete EMS v2.0.
- Deploy Fire Grants Review/Award V4.30 to production.
- Implement process improvement for software development projects and execute project reviews Implement MS Project Server 2007.
- Complete project to limit to three failed login attempts to database.
- Develop Personally Identifiable Information Application & database.
- Develop Real Property Management Application.

- Develop Real Property Management E-Dashboard.
- Implement Tower TRIM (Mitigation Electronic File Storage).
- Implement Travel Manager v9.0.
- Complete consolidation of training database.

2007 USCIS Accomplishments

- Integrated seven legacy enterprise applications through a Service Oriented Architecture Enterprise Service Bus improving information access and sharing with another Federal Department.
- Implemented and instituted the USCIS information technology lifecycle management process.
- Implemented and instituted an Office of Information Technology organizational structure based on the industry best practice model of information technology infrastructure library and information technology service management.
- Received Departmental approval for USCIS's Transformation Program Concept of Operations and Strategic Plan and the Transformation Program for Milestone Decision Point (MDP) two – Concept and Technology Development Phase.
- DHS' Enterprise Architecture Community of Excellence approved USCIS Transformation Program for Milestone Decision Point two – Concept and Technology Development Phase.
- USCIS Transformation Program Office (TPO) completed foundational documents to support the Program Management Office including: Program Management Plan,
- Governance Plan, Risk Management Plan, Quality Management, Change Management Plan, and Communication Plan.
- Initiated Federal Stakeholders Advisory Board that includes members from: CBP, USCIS, I&A, Department of Justice, Department of State, ICE, Treasury, and US-VISIT.
- Completed the Transformation Increment 1 Target Business Process definition which defines the business model and high-level requirements for the program.
- USCIS TPO completed initial round of field briefings and focus group meetings with field leadership.
- For the pilot projects, the TPO engaged users through focus groups and surveys to gather and validate requirements, validate new business processes, and collect feedback for future requirements.
- Deployed three pilot projects – Secure Information Management Service, Enterprise Document Management System, and Enumeration.

USCIS Remaining Plans

- Complete procurement of Solutions Architect services.
- Begin development of integrated operating environment.
- Complete hiring process to staff Enterprise Architecture Branch with the USCIS Office of Information and Technology.
- Execute USCIS EA development plan to achieve level three maturity.

- Facilitate USCIS-wide performance architecture task force to gather and analyze performance measures and metrics

FY 2007 Challenge 6: Infrastructure Protection

Summary of 2007 Challenge: OIG acknowledged that the Nation's distribution of critical infrastructure and key resources (CI-KR) is enormous and complex. The requirement to rely on Federal partners and the private sector to deter threats, mitigate vulnerabilities, or minimize incident consequences complicates protection efforts for all CI-KR. However, according to OIG, the Department continues to face a challenge in prioritizing its protection efforts based on risk and mission requirements and needs to incorporate threat information into its risk assessments and coordinate the funding of protective measures for CI-KR.

2007 Accomplishments

The Department of Homeland Security's Office of Infrastructure Protection (OIP) is responsible for coordinating and advancing protection efforts throughout all 17 critical infrastructure and key resource sectors:

- The completion of the National Infrastructure Protection Plan's Sector Specific Plans (SSPs) is just one of many OIP activities that illustrate the evolution of the Department's CI-KR protection capabilities. This undertaking represents the first time that government and the private sector have worked together on such a large scale to develop a joint plan for protecting the Nation's key assets and resources. In completing the SSPs, DHS:
  - Worked with the private sector to implement tailored protective measures, including conducting site-assistance visits and transforming feedback into educational reports that owners and operators can use to identify vulnerabilities;
  - Worked with the private sector to develop more than 800 Buffer Zone Protection Plans (BZPP) to enhance security around critical infrastructure;
  - Provided security guard training and courses on increasing terrorism awareness; and
  - Boosted information sharing across the sector through the Homeland Security Information Network (HSIN), which has a specifically dedicated portal for critical infrastructure.
- More work continues in these different sectors. For example, in the chemical sector, DHS issued an Interim Final Rule for Chemical Facility Anti-Terrorism Standards in April 2007. The Department is now finalizing the final rule, ensuring vulnerability assessments are conducted, and fostering the development of site security plans. OIP also began sector-wide registration processes in the Nuclear, Oil and Gas, and Chemical Sectors to clearly identify all owners and operators.
- Sharing information on threats in the form of tailored strategic sector-specific risk assessments, vulnerabilities, consequences, and protective planning was an essential underlying foundation for executing these activities and completing these deliverables.
- Because strategic information motivates protective investments and preparedness, the National Infrastructure Protection Plan (NIPP) Sector Partnership Model, which is fully operational, has been and will continue to be an essential mechanism for the exchange of

strategic information at an unprecedented level between government and the owners and operators of CI-KR.

- The National Infrastructure Coordinating Center (NICC) has taken important strides in the realm of information sharing. Consistent with the NIPP "network approach" to information sharing, the NICC routinely shares a wide range of information products containing warning, threat, and CI-KR protection information via HSIN-Critical Sectors (HSIN-CS). During the last year, the NICC has posted more than 900 information products to HSIN-CS for use by CI-KR owners and operators.
    - Nine of the CI-KR sectors or major sub-sectors have signed MOUs with DHS to deploy HSIN-CS to their sectors, which reflects a long process to overcoming challenges unique to information sharing with the private sector.
    - This comprehensive environment and its mechanisms have been formally adopted by the Program Manager, Information Sharing Environment (PM-ISE), as the private sector component of the information sharing environment.
- The Buffer Zone Protection Program reduces the threats and vulnerabilities for critical infrastructure through identification and analysis of critical infrastructure sites and by providing grant funding to law enforcement entities to mitigate identified gaps. DHS is documenting, through the Vulnerability Reduction Purchasing Plan (VRPP), how BZPP grantees are utilizing the grant money to reduce threat and vulnerabilities.
    - OIP provided $25 million of BZPP grant funds for increased local law enforcement (LLE) capability to protect the buffer zones around high-risk chemical facilities.
    - OIP completed 200 Buffer Zone Plans and provided $50 million in BZPP grant funds for increased LLE capabilities.

In addition, OIP:

- Completed 110 Site Assist Visits (SAVs) in conjunction with Federal, State, local, and private-sector stakeholders.
- Completed the remaining 28 (of 65 total Nuclear Power Plants) Nuclear Comprehensive Reviews (CRs).
- Completed the remaining 5 of (6 total high-risk chemical regions) Regional Chemical CRs.
- Completed 130 Soft Target Awareness Courses to LLE and private sector security managers.
- Completed 50 Surveillance Detection Courses to LLE protecting the CI-KR.
- Completed FY 2008 Tier 2 Data Call for infrastructure information with States and SSAs.
- Achieved initial operating capability of iCAV system to provide situational awareness within the National Operations Center.
- Completed the 2007 National and Sector CI-KR Protection Annual Reports in accordance with the NIPP.
- Initiated and completed the 2007 NIPP CI-KR Protection Core Metrics Initiative to include NIPP and OIP implementation actions.

Remaining Plans

DHS will continue to prioritize resources and activities based on risk. In addition, OIP will:

- Develop a scalable assessment methodology to execute SAVs, Buffer Zone Protection Plans, Comprehensive Reviews, and High-Risk Infrastructure Cluster Assessments. This represents an important step in working with other Sector Specific Agencies to standardize assessment methodologies while fulfilling bombing prevention requirements, providing accessibility to State and local partners, and allowing Protective Security Advisor-led assessment teams to coordinate and report on vulnerability assessments in the field.
- Integrate 10 National Guard teams into the Vulnerability Assessment project and conduct approximately 300 vulnerability assessments on Tier 1/2 CI-KR. The National Guard will test, evaluate, and calibrate the new methodology.
- Conduct the high-risk cluster assessment pilot on 72 assets in the Lower Manhattan Security Initiative and 24 assets in the District of Columbia Metroplex Initiative. These assessments will allow OIP to evaluate and enhance the methodology to conduct full scale High-Risk Infrastructure Cluster assessments in following years.
- Expand the CR effort to conduct assessments for high-consequence sectors such as liquefied natural gas.
- Establish a Protective Measures Section to track Federal, State, and local government and private sector assessments and protective actions. This section will collect and analyze information to evaluate the effectiveness of assessments, protective measures implemented, and grant funding provided to high-priority CI-KR.
- Evolve the National Asset Database into an integrated Infrastructure Data Warehouse (IDW) with raw CI-KR-related asset information and completed CI-KR information products. All NIPP Stakeholders will have access to the IDW via a common graphics user interface.
- Review, as requested, sector-specific risk assessment methodologies to ensure NIPP compliance, and then assist with the technical implementation of the tool for use in the collection and assessment of sector-level CI-KR.

FY 2007 Challenge 7: Border Security

Summary of 2007 Challenge: The OIG letter asserts that one of DHS' primary missions is to reduce America's vulnerability to terrorism by controlling the borders of the United States. This is dependent on the coordinated accomplishments of DHS, as well as joint efforts with other agencies. To this end, DHS is implementing a comprehensive multi-year plan to secure the borders and reduce illegal immigration, called the Secure Border Initiative (SBI). OIG believes that DHS must quickly establish the organizational capacity to oversee, manage, and execute a program of this size and scope. Until the operational and contract requirements are firm, effective performance management and cost and schedule control are precluded. Concurrently, CBP must increase the number of agents by 6,000 in less than three years. The rapid timeline presents risks in recruiting and training fully qualified agents and procuring the necessary infrastructure to support them.

2007 Accomplishments

Fielding Border Surveillance Technologies / SBI*net* Program Management

- CBP awarded an SBI*net* task order to demonstrate the effectiveness of the overall approach to SBI*net* along 28 miles of border flanking the Sasabe Port of Entry (POE) in Arizona. CBP has made significant progress in implementing Project 28, including deploying all nine re-locatable camera and radar towers, and fitting all 50 of the Project 28 agent vehicles with Common Operating Picture hardware.
- Under the SBI*net* prime contract, CBP awarded a task order for the test and evaluation of fencing solutions. The purpose was to test effective low-cost solutions that meet operational requirements and can be reproduced for rapid deployment along the Southwest Border. This testing will help CBP add to existing tactical infrastructure to reach a total of 370 miles of fencing and 200 miles of vehicle barriers by the end of calendar year 2008.
- CBP met its commitment to construct 70 miles of primary fencing along the Southwest Border. This effort was comprised of both new and previously planned projects brought together under SBI*net*.
- CBP formed a Secure Border Initiative (SBI) Executive Steering Committee (ESC) to provide oversight of the implementation of SBI and SBI*net*. The SBI ESC serves as an advisory board, helping the SBI Executive Director to effectively implement program management decisions.
- SBI is developing, documenting, and implementing sound program and performance management processes. SBI developed a process asset library, with a baseline of 76 program management policies, plans, processes, and procedures. The program has established scheduling standards for the development and maintenance of the Integrated Master Schedule and project schedules. SBI has established processes and procedures for Earned Value Management System baseline analysis and reporting. Monthly Program Management Reviews, which address cost, schedule, performance, and risk – are conducted to monitor the program progress. Oversight of Prime contractor deliverables are performed to ensure measures and metrics reported are consistent and traceable to the Quality Assurance Surveillance Plan (QASP). .
- SBI and SBI*net* have significantly increased organizational capacity, adding 168 staff members to help manage the program and address crosscutting issues such as coordination with the Coast Guard on maritime border security issues.

Office of Border Patrol

- OASISS (Operation Against Smugglers Initiative for Safety and Security) has been embraced and expanded by both the U.S. and Mexico as a successful cross-border prosecution and deterrent to smugglers who jeopardize the lives of aliens.
- 311 cases were generated, a 9 percent increase over FY 2006, with an 86 percent acceptance rate.
- Interior Repatriation (13,292 aliens were removed via this program) along with OASISS has complimented the Border Security Initiative campaign to inform and deter potential crossers.
- Operation Streamline has decreased Del Rio Sector apprehensions by 47 percent (and Other Than Mexican (OTM) apprehensions by a similar 46 percent).

- Nationwide apprehensions were down 19.5 percent for FY 2007 to 876,704.
- Nationwide apprehensions of OTM nationalities were down 37 percent to 68,016.
- 59,146 OTM aliens have been removed through the Expedited Removal (ER) program helping to end Catch and Release.
- In FY 2007, CBP significantly increased the number of Border Patrol Agents from 12,319 to 14,923 agents as part of the President's initiative to increase the ranks of the Border Patrol by 6,000 by December 31, 2008.
- The Border Patrol Academy participated in a curriculum review with the Federal Law Enforcement Training Center before initiating a new 81-day program.
- As of September 30, 2007, 1,712 agents have graduated from the Academy with 1,442 FY 2007 recruits still in class. This is a single year record for graduates at the Academy. To accomplish this goal the Academy doubled the size of permanent staff and has increased the number of temporary duty instructors. The infrastructure at the Artesia Academy was improved to meet the need; a new dorm, physical techniques training center, modular classrooms, and other additions have been made.
- The Academy has, with input from best in practice practitioners and from field Border Patrol Agents, designed a new Spanish language program and physical techniques training program. The redesign will ensure that new Agents who are already proficient in Spanish can complete the basic training at the Academy in 55 days. Those needing Spanish, will enter a 40 day task-based Spanish program.
- Planned for 6,000 new agents by December 31, 2008. Conducted site surveys of existing stations. Identified facility conditions and needs of each station receiving additional agents.
- Environmental kick off meeting conducted with environmental contracting firm on September 25, 2007 for all Integrated Project Team (IPT) projects. Environmental Assessments (EAs) to start immediately on identified sites.
- Initiated land acquisition activities for Rapid Response sites.
- Execution underway for several Rapid Response projects.
- Completed Rapid Response Planning IPT activities in April 2007. Outputs included initial cost estimates and program of requirements for all Rapid Response sites, prioritized list of projects, programmatic cost benefit analysis, risk management plan, and mission needs statement.
- Implemented cost and schedule management system for Rapid Response projects.
- Completed BP facilities for 12 sites.
- 36 renovations, additions, upgrades, and/or new facilities were completed in various locations.
- 184 acres acquired for five facilities.

Advance Passenger Information System (APIS)

- On August 23, 2007, the APIS Pre-Departure Final Rule, requiring air and vessel carriers to transmit complete APIS manifest data prior to sealing the aircraft doors or the departure of a vessel, was published in the *Federal Register*. This rule enables CBP to conduct no fly and selectee watch list screening prior to passengers gaining access to the aircraft or departing onboard a vessel, adding an essential layer to our anti-terrorism

security measures. Carriers have been given 180 days from the publication of the rule to transition their systems into compliance.

- On September 18, 2007, the CBP Private Aircraft Notice of Proposed Rule Making, requiring pilots of private aircraft to transmit complete APIS manifest data 60 minutes prior to departure was published in the *Federal Register*. This rule enables CBP to conduct no fly and selectee watch list screening and provide Landing Rights for Private Aircraft through an automated system, adding an essential layer to our anti-terrorism security measures.

Intelligence

- Developed a complete Field Intelligence Construct, and successfully validated it through a six month, Tucson, Arizona-based Pilot focused on the Southwest Border. This initiative integrates with and compliments the Border Security and Intelligence aspects of the SBI*net* Program.
- Developed a Strategic Threat Assessment Program and completed first assessment on the threat posed by Terrorism at the CBP Ports of Entry.
- Refined the Passenger Targeting Rules Set, resulting in increased focus on problematic passengers, and a reduction in delays and secondary screening of unlikely terrorists and other criminals.

ICE/CBP Coordination

- The ICE Office of Intelligence has successfully completed a Headquarters reorganization that will foster and enhance the strategic collaborative efforts between ICE and CBP, as well as other DHS entities.
- The Office of Intelligence has successfully completed a field reorganization that will greatly enhance our ability to meet the intelligence needs of ICE and our customers, which includes CBP. The Office of Intelligence has transitioned from six regional Field Intelligence Units (FIUs) and is in the process of replacing them with 26 Field Intelligence Groups that are co-located with ICE offices in the field. This will better facilitate information sharing between ICE and CBP Intel.
- CBP and ICE use shared database resources to exchange information, reports, and other operational and intelligence information on subjects of common interest.
- The Coordination Council affords ICE and CBP senior executives the opportunity to openly discuss each respective agency's roles and responsibilities. Through the Coordination Council, ICE and CBP were able to jointly develop an addendum to the November 16, 2004, joint memorandum between ICE/OI and CBP/OBP. This document highlights efforts to promote occupational awareness and orientation among field elements of ICE and CBP personnel. These efforts will include the respective ICE/OI and CBP/OBP entities providing orientation to each other's personnel on operational priorities, programmatic areas of concern, evidence handling and other related matters. The addendum specifically addresses the co-location of ICE OI and CBP OBP Sector Intelligence Units where building space limitations can be overcome.

Remaining Plans

Fielding Border Surveillance Technologies / SBI*net* Program Management

- CBP is committed to build a total of 370 miles of fence and 200 miles of vehicle barriers along the Southwest Border by the end of calendar year 2008.
- CBP is committed to deploying 70 communications, camera, and radar towers by the end of calendar year 2008.

Office of Border Patrol

- Extend Operation Streamline-like initiatives to other Border Patrol Sectors.
- Continue to refine the use Interior Repatriation and the OASISS program to deter at risk crossers.
- Continue to expand the use of ER to more eligible classes of aliens and in more geographic locations.
- The Border Patrol will further improve the Academy training program.
- The Academy plans to conduct 96 classes for a total of 4,800 trainees.
- Continue 55 Rapid Response program projects currently underway.
- In FY 2008, complete Border Patrol facilities for eight locations.
- Complete Northern Border standard, 50 agent standard station design.
- New construction activity underway in six sectors.
- Continue activity with offers pending with an estimated value of $3.8 million, for six site locations, totaling 123 acres.

Advance Passenger Information Systems (APIS)

- Monitor carrier compliance/implementation progress of requirements defined in the APIS Pre-Departure Final Rule.
- Finalize and publish the CBP Private Aircraft Final Rule upon analysis and reconciliation of comments received from the Notice of Proposed Rule Making.

Intelligence

- Deploy 2-3 Intelligence and Operations Coordination Centers and 6-10 Intelligence Coordination Teams to Border locations over a 24-month time frame commencing October 1, 2007. These are the key structural elements of the Field Intelligence Construct.
- Complete build out of the Strategic Threat Assessment Program to encompass All Crimes/All Threats; integrate programmatically into the new CBP Integrated Strategic Planning and Resource Allocation Process; and develop Indicators and Warning capability based on this program to provide, in concert with our mission partners, a first-ever Predictive Capability for All Crimes/All Threats.
- Enhance CBP Leadership and Mission Partner Situational Awareness by combining the Intelligence Watch and the Operations Situations Room conceptually and under one leader.

ICE/CBP Coordination

- In furtherance of the goal of closer collaboration and sharing of law enforcement intelligence, CBP and ICE Intel also recently agreed to produce coordinated joint reporting to meet the analytical needs of both agencies. This will be a joint ICE and CBP Office of Intelligence analytical effort dealing with border activity of mutual interest to both agencies. The focus will be on analyzing regional and national smuggling trends, methods and seizures and combining it with all-source intelligence to provide trend analysis that directly relates to ICE and CBP operations in the air, land and sea.
- Environments of interest to both ICE and CBP field level personnel as well as managers at both agency headquarters.
- ICE and CBP are currently discussing the shared use of ICE data systems that will allow both agencies to conduct useful analysis on differing data sets.
- Intelligence dissemination measures and initiatives are underway. The DHS Intelligence Systems Board aims to unify the intelligence program throughout DHS through an enterprise approach to information sharing and the application of common systems.

FY 2007 Challenge 8: Transportation Security

Summary of 2007 Challenge: The OIG's letter acknowledged that the size and complexity of the transportation system, which moves millions of passengers and tons of freight every day, make it a difficult system to secure and an attractive target for terrorists. The Nation's economy depends upon implementation of effective, yet efficient transportation security measures. The OIG claimed however, that since its inception, TSA has focused almost all of its attention on aviation security, perhaps to the detriment of other forms of transportation.

Checkpoint and Checked Baggage Performance

2007 Accomplishments

Screening SOP Refinements

- TSA has undertaken a number of initiatives in 2007 to improve checkpoint and checked baggage performance. Screening SOPs continue to be refined to shift attention from lower security risks, such as lighters, to address markedly higher security risks that could do catastrophic damage to an aircraft—IEDs, IED parts, and electric ignition devices. This focus is fundamental to a risk-based approach to aviation security. TSA continues to direct resources toward higher risk areas and make its security protocols less transparent to potential terrorists. We believe we gain a higher return in threat detection when our TSOs concentrate on finding explosive devices or components of explosive devices.

Screener Performance

Aviation Screening Assessment Program (ASAP)

- In order to improve screener performance, TSA instituted ASAP in 2007. The mission of ASAP is to measure screening performance using realistic and standardized assessment scenarios to improve aviation security. This is being accomplished by:

  - Establishing a three-tiered assessment system with standardized criteria and menu-driven scenarios;
  - Conducting on-going evaluation and modification to the program and scenarios;
  - Utilizing the local screening workforce including TSA Approved Instructors (TAI) and Bomb Appraisal Officers (BAO) as subject matter experts;
  - Integrating the program plan into the Transportation Security Inspector (TSI) Annual Inspection Plan; and
  - Providing clear and consistent communication to the field.
- The program's main goal is to achieve a national assessment measurement. This measurement provides information that helps TSA improve aviation security and identify vulnerabilities across screening operations.

Performance Accountability and Standards System (PASS)

- The objective of PASS is to promote and sustain a culture of high performance and accountability in TSA and to help achieve the organizational goals that support TSA's mission. PASS is designed to ensure that employees know what they need to do to accomplish their work successfully and to help TSA accomplish its mission through the use of a pay-for-performance system. PASS begins with a sit-down face-to-face planning meeting between employees and their supervisors or managers at the beginning of the performance period. At the end of the first and third performance quarters, quarterly discussions are held. A Mid-Year Review occurs halfway through the performance period, and the performance period wraps up with an End-of-Year Review.

Emerging Technologies

- TSA continues its efforts to identify and deploy emerging technologies that will constitute the next advancement in explosives detection screening at passenger security checkpoints. Those emerging technologies that are either in, or will soon be ready for, operational evaluation in screening for explosives includes: (1) Cast & Prosthesis scanners, (2) Whole Body Imagers, (3) bottled liquids scanners and (4) advanced carry-on baggage scanning technologies.

Additional Layers of Security

Aviation Direct Access Screening Program (ADASP)

- TSA is implementing ADASP as one more layer of protection against terrorism. Recent incidents in the United States and overseas have highlighted vulnerabilities that exist with regard to individuals with unescorted and unscreened access to secured areas and sterile areas of airports. Increased random inspections of individuals, accessible property, and vehicles entering secured areas and/or sterile areas are required to reduce the risk from these vulnerabilities.

Visible Intermodal Protection and Response (VIPR)

- To help combat threats such as the one experienced in Glasgow, TSA instituted VIPR, a visible deterrent to terrorist activity. VIPR consists of Behavior Detection Officers, Federal Air Marshals, Explosives Detection Canine Teams, Transportation
- Security Inspectors, and State and local law enforcement officers, who operate throughout the airport environment as an additional layer of security.

Remaining Plans

- To meet the challenges of a constantly evolving threat, our passenger screening systems must constantly evolve and adapt. To this end, TSA created a passenger screening task force charged with creating a new vision for aviation passenger screening. A vision that will enable TSA to focus more on high-risk individuals, that expands the range of threats that can be detected, that enables the information sharing across the enterprise, and that improves our system's ability to respond to ever-changing threat conditions. The task force has established guidelines for the development of the passenger screening system vision of the future. Next steps include integration of these guidelines and working with stakeholders, such as airports, to bring the concepts to fruition.

Passenger Air Cargo Security

2007 Accomplishments

- TSA has removed exemptions to screening to include the elimination of shrink wrap exemptions. In addition, TSA holds four weeks of core inspector training. Cargo Inspectors complete a two-week on-the-job training program. TSA's more than 460 canine teams each spend at least 25 percent of their work day in the cargo environment.

Remaining Plans

- TSA will plan direct nighttime and weekend inspection activities (when most of the cargo is moving) to better determine compliance with requirements, and conduct monthly "cargo strike" surges at high volume cargo airports. By the end of FY 2008, TSA will add another 170 canine teams to the force who's primary focus will be cargo, which will significantly increase the amount canine teams screening cargo.

Worker's Compensation

2007 Accomplishments

- Developed agency policies and procedures on the FECA program to include roles and responsibilities for the Office of Human Capital (OHC) and airport personnel.
- Developed and implemented a centralized, automated case management system to track the status of the Agency's workers' compensation cases.
- Provided 40 positions in which to concentrate exclusively on the Workers Compensation program in field locations.

- Developed and implemented FECA related performance goals and measures, and established performance standards for workers' compensation specialists and Federal
- Security Directors (FSDs) that will hold TSA officials accountable for program performance.
- Developed agency policies and procedures on TSA's chargeback process to include roles and responsibilities for OHC and airport personnel. Additionally, the verification process of reviewing and verification of the Chargeback Cost has been added to the *Workers' Compensation Desk Guide.*

Remaining Plans

- Finalize the Management Directive outlining roles and responsibilities for the FECA program, and continue to communicate the fact that locations should use the case management system and provide associated training.

Employee Workplace Issues

2007 Accomplishments

- TSA's Equal Employment Opportunity complaints are comparable to other deferral agencies. TSA's attrition is decreasing and is comparable to other transportation sector jobs. Additionally, TSO job satisfaction has increased significantly over the past two years. TSA has multiple processes for complaint resolution including the Ombudsman's Office, the Office of Civil Rights, Disciplinary Review Board, and Peer Review Programs. TSA has established a Model Workplace Program where employees and managers form councils to address workplace complaints and grievances.

Remaining Plans

- OIG is currently conducting an audit of employee workplace issues. At the conclusion of the OIG audit, TSA will review and address the identified findings and recommendations.

Rail and Mass Transit

2007 Accomplishments

- DHS has developed and administered grant programs for various surface transportation modes.
- Developed and adopted a strategic approach for implementing surface transportation security functions.
- Conducted threat, criticality, and vulnerability assessments of surface transportation assets.
- TSA has taken actions to develop and issue surface transportation security standards for passenger and freight rail modes.
- TSA has taken steps to conduct compliance inspections for surface transportation systems and has made progress in hiring and deploying inspectors.

Remaining Plans

- OIG and GAO are both conducting audits in this area. At the conclusion of the audits, TSA will review and address the identified findings and recommendations.

FY 2007 Challenge 9: Trade Operations and Security

Summary of 2007 Challenge: OIG states that trade operations and security are primarily the responsibility of CBP, although USCG and ICE also play important support roles. CBP has the mission of ensuring that all persons and cargo enter and exit the U.S. legally, while facilitating the lawful movement of goods and persons across U.S. borders. OIG believes CBP's three major challenges to meeting its trade mission are the modernization of trade systems, risk management programs to use scarce resources efficiently, and partnerships with the trade and foreign Customs offices.

2007 CBP Accomplishments

Container Security Initiative (CSI)

- Reached a milestone of 58 Operational CSI ports, covering 86 percent of U.S. bound maritime containers.
- Transitioned 12 CSI ports in eight countries to permanent staffing, bringing the total number of posts with permanent personnel to 40.
- Increased the level of examinations conducted at CSI locations by 92 percent.
- Evaluated 40 CSI ports using automated tools and protocols.
- Launched Secure Freight Initiative (SFI).

Cargo Enforcement Reporting and Tracking System (CERTS)

- The CERTS examinations and findings module, a component of Automated Targeting System, Version 4 (ATS-4), was actively deployed during FY 2007. This new module enables CBP Officers and Agriculture Specialists to report and track all CBP examinations and findings data using a single-point of entry application.
- ATS-4/CERTS is currently deployed to 36 CBP seaports, five CBP Airports, and two SFI seaports (Port Qasim, Pakistan and Port Cortes, Honduras).
- Thirty international airports have just finished sending representatives to the CERTS Train-The-Trainer Course.

Customs-Trade Partnership Against Terrorism (C-TPAT)

- Initiated 2,503 validations of which 1,812 have been completed, resulting in 5,314 total validations completed.
- Increased to a total of 156 Supply Chain Security Specialists (SCSS) positions.
- Implemented a third party validation pilot program and achieved several milestones to include: (1) soliciting applications from companies wanting to conduct validations on behalf of CBP in China on the Federal Business Opportunities Website and selecting 11

companies to participate; (2) identifying and inviting 304 validated importers to participate in the pilot; and (3) developing standard operating procedures to ensure consistent application of validation principles.
- Strengthened supply chain security through the development and issuance to the trade community of minimum-security criteria for U.S and Foreign-Based Marine Port Authority and Terminal Operator, Licensed U.S. Customs Brokers, Mexican Long Haul Carriers, and Air Carriers.

Automated Commercial Environment (ACE)
- Deployment of truck e-Manifest was completed at all land border cargo crossings (105 port codes, 144 sites).
- ACE e-Manifest, as required by the Trade Act of 2002, advance electronic cargo information mandate, was deployed at all ports by November 2007. The use of ACE e-Manifest became mandatory in Maine and Minnesota on October 12, 2007 and will become mandatory in Alaska on February 11, 2008.
- Ports with ACE truck e-manifest capabilities are operating at a compliance rate of nearly 100 percent.
- CBP collected nearly $1 billion dollars in duties and fees via the ACE periodic monthly statement payment process, which represents 36 percent of all duties and fees collected.
- Currently, there are 12,265 ACE accounts (10,189 truck carriers, 1,306 importers, 770 brokers, filers and sureties).
- ACE truck manifest capabilities are operating at 98 or 99 land border ports; the mandatory e-Manifest policy is in effect at 79 land border ports.
- Deployed initial ACE entry summary, accounts, and revenue capabilities on September 9, 2007.
- More than 245 users from 35 participating Government agencies are using ACE to access trade data, including more than 100 reports that draw from entry and entry summary data.
- Periodic monthly statement receipts grew to $1 billion, representing 42 percent of total adjusted collections. Overall, there are nearly 12,000 ACE Secure Data Portal accounts, and more than 8,000 corporate entities approved to pay duties and fees monthly.
- CBP achieved the planned target for the ACE Critical Few performance measures, based on the CBP Performance Reference Model (PRM), that track the number of ACE accounts, the percentage of duties and fees paid via the ACE periodic monthly statement process, the national percentage of e-Manifests filed, and the percent of reduction in truck processing time due to e-Manifest filing.
- CBP continues to fine tune ACE truck processing capabilities and is working to address and resolve system defects. The completion of computer hardware upgrades that were being performed during the survey period have resulted in officers at several ports reporting a remarkable improvement in ACE processing speed. A recent consolidation of system databases addressed previous system problems that often necessitated multiple system queries to obtain truck-related information, and since the consolidation, ACE has consistently provided officers with immediate access to this data. CBP also developed a portal-generated "cover sheet" that can be used by carriers as proof of filing an e-Manifest during system down times.

- CBP continues efforts to improve the availability and responsiveness of ACE user support, as well as communications to users and stakeholders regarding system status. Efforts taken to date include increasing help desk staff, referring more complicated inquiries to a higher tier of support, using automated phone messages to alert callers to system problems, and developing a communications plan for the immediate notification of ACE status to users and stakeholders. CBP held a National Truck Manifest Conference to brief CBP field staff on deployment, share lessons learned, and discuss both standard operating procedures and the aforementioned user satisfaction survey.

ATS Targeting Rule Revisions/Automated Targeting System: CBP Targeting Efforts/Initiatives

- Developed and implemented a new weight set for security targeting of ocean cargo. In addition the weight set performance is monitored and adjusted by incorporating identified seizures into the proxy positive set utilized in the Receiver Operating Characteristics rule performance model.
- CBP has designed, developed, and deployed the Mock Shipment Module. This module provides a platform for the development of scenario based shipment and evaluation of rule performance.
- Implemented with the U.S. Postal Service to utilize an automated targeting solution for outbound mail.
- Implemented a process to extract examination data, analysis shipment findings data, compare targeted shipments findings data utilizing Receiver Operating Characteristics (ROCs), conduct impact assessments, and modify rules and weight sets as need to increase targeting effectiveness.

Office of International Trade

- Organized the trade functions resident in three different CBP offices into one Office of International Trade.
- Signed a Memorandum of Cooperation with China on intellectual property intended to reduce China's export of counterfeit goods.
- Increased intellectual property seizures by 22 percent to 7,245 (323 of which have a nexus to health and safety) with a value of $110 million, a year-on-year increase of 141 percent.
- Published an updated System of Records Notice, under the Privacy Act, and a Notice of Proposed Rulemaking for Privacy Act Exemptions in the Federal Register, and posted a revised Privacy Impact Assessment on the DHS web site for the Automated Targeting System (ATS). ATS is the premier tool employed by DHS and CBP to screen and vet, in advance, both persons, coming to and departing from the United States, and all cargo entering or exiting U.S. Commerce. The publication of this separate System of Records Notice and Privacy Impact Assessment for ATS permits CBP to ensure protections for individual privacy while contributing to the achievement of DHS' principal mission of preventing and deterring terrorist attacks. The ATS System of Records Notice and Privacy Impact Assessment establish strict time limits for the Government regarding the retention of personal or identity information belonging to international travelers and afford those same travelers the means to obtain access and correct the information that the CBP has collected about them and their travel itinerary.

- Enhanced the development of the ACE project by drafting and publishing Federal Register Notices that expanded the implementation of ACE e-manifest for trucks to all the land border locations and mandated the use of ACE e-manifest for trucks at all land border locations except for ports in Alaska.
- Supported the development of ACE by publishing Federal Register Notices that established formal terms and conditions for participation of trade members in the ACE test, increased the number and type of merchandise that can be released from CBP off the ACE e-manifest for trucks, and allowed third-party service providers to submit e-manifest information in the truck environment.
- A final rule requiring United States citizens and nonimmigrant aliens from Canada, Bermuda, and Mexico departing from or entering the United States from within the Western Hemisphere at air ports-of-entry to present a valid passport was published on November 24, 2006 in the *Federal Register*.
- A final rule requiring that electronic manifest information for passengers on board commercial aircraft arriving in and departing from the United States and passengers and crew onboard arriving and departing commercial vessels (with certain exceptions) be vetted by DHS against a government-established and maintained terrorist watch list prior to departure of the aircraft or vessel was published on August 23, 2007 in the *Federal Register*.
- Issued regulations implementing several Free Trade Agreements, including U.S. agreements with Chile, Singapore, Jordan, and Morocco.

Remaining CBP Plans

Container Security Initiative (CSI)

- Maintain 58 CSI ports, continuing coverage of 86 percent of containerized cargo destined to the United States.
- Train personnel to work with and support the Secure Freight Initiative (SFI).
- Evaluate remote targeting pilot project with real-time remote imaging and live video of the inspectional process.

Cargo Enforcement Reporting and Tracking System

- Deployment to all U.S. seaports and airport, the 58 CSI ports and the one remaining SFI port (Southampton, UK).

Customs-Trade Partnership Against Terrorism

- Conduct approximately 3,500 validations in FY 2008
- Finalize personnel actions to staff new offices in Buffalo, New York and Houston, Texas.
- Seek to finalize two additional Mutual Recognition Arrangements.

Automated Commercial Environment (ACE)

- Develop new ACE capabilities to strengthen screening and targeting.
- Complete deployment of ACE truck processing capabilities and expand the mandatory e-Manifest policy.

- Continue development of new ACE capabilities that will further strengthen border security and streamline operations for CBP officers and the trade community.

2007 USCG Accomplishments

The USCG continued to mature its Ports, Waterways, and Coastal Security (PWCS) program increasingly focusing on risk based measures and maximizing effects. Some key port security accomplishments include:

- The Coast Guard updated its operations order for Operation NEPTUNE SHIELD, which directs and guides field implementation of the PWCS mission. A few examples of recent improvements include:
  - Risk-based patrol activity: Improved effectiveness and efficiency of surveillance patrols by focusing patrol activity near maritime CI-KR at greatest risk, leveraging the Maritime Security Risk Analysis Model (MSRAM);
  - Risk-based escorts: Focused escorts on vessels laden Especially Hazardous Cargoes rather than all Certain Dangerous Cargoes;
  - Increased availability of aerial assets to conduct patrols and escorts increased USCG presence and reduced the threat of adversary planning; and
  - Prioritizing Security Activities: Emphasized execution of activities that produced greatest reductions in maritime risk and aligned resource usage on this risk based approach.
- Refined High Interest Vessel targeting matrix to focus boardings on vessels with highest risk.
- USCG commissioned two Maritime Force Protection Units, funded by the Navy, to provide dedicated security to transiting SSBNs and free up other USCG assets to perform other homeland security and non-homeland security missions.
- Engaged with small vessel community thru the June 2007 DHS National Small Vessel Security Summit to identify ways to mitigate risk associated with small vessels (< 300 Gross Tons).
- USCG Atlantic Area Commander and USN Commander Second Fleet developed a Homeland Security – Homeland Defense Concept Plan.
- Verified compliance with Vessel and Facility Security Plans through announced and unannounced spot checks and inspections
- USCG completed two Waterways Suitability Reports for LNG facilities in FY 2007.
- Underwater Terrorism Preparedness Plans (UTPPs) have been developed and delivered to 17 major ports. The goal of this program is to deliver actionable plans that local (field level) USCG commanders can use to readily access information about underwater capabilities and coordination mechanisms in their Area of Responsibility (AOR) to prevent, detect, and respond to an underwater threat. UTPPs are locally developed preparedness plans that establish preventive measures to make it more difficult for terrorist to conduct underwater surveillance or launch underwater attacks in and around our Marine Transportation System (MTS). Because if the complexity, scope, and potential consequences of an underwater terrorist event, UTPPs focus on preparedness of port partners through communications, coordination, enhanced awareness of potential

threats, and clear delineation of roles and responsibilities in enhancing underwater security.
- USCG reorganized its deployable response capabilities under the Deployable Operations Group streamlining response capabilities of specialized teams and equipment to meet the Department's all hazards protect and respond requirement.
- USCG made significant improvements in National Maritime Strategic Risk Assessment (NMSRA), which enhances the utility of MSRAM.

Remaining USCG Plans

- The Coast Guard is in the final stages of review and prepared to publish an updated version of *Combating Maritime Terrorism.* This campaign plan details the way ahead for the PWCS mission and further expounds upon maritime governance, the Coast Guard's three-pronged approach to protecting the Nation's ports and waterways. As the *Combating Maritime Terrorism* plan matures, activities will be refined, risk reduction numbers will be validated, and the Coast Guard will leverage its DHS lead Federal agency role to provide a more comprehensive maritime risk reduction strategy.
- The Coast Guard leads an interagency group developing the National Strategy for Small Vessel Security that specifically examines and addresses the threats small vessels pose to free and smooth maritime commerce.
- The Coast Guard is consolidating the documents, policies, and procedures that encompass port security into a concise manual that provides direction to field units in the successful protection of the Nation's ports and free and smooth maritime commerce.
- The Coast Guard is developing implementation plans for an aggressive weapons training policy that maximizes technologies, reduces costs, is more environmentally friendly, and reduces risk.
- Maritime Force Protection Units: The first dedicated vessel arrives at Kings Bay, Georgia, in December 2007 and second arrives at Bangor, Washington, in April 2008.
- The Coast Guard made significant progress in FY 2007 toward updating Area Maritime Security Plan and Area Maritime Security Committee guidance. Through an inter-agency working group this plan will include implementation of the new SAFE Port Act (Section 101) requirements for a Salvage Response Plan to support expeditious post-TSI resumption of commerce. It also will assist in the implementation of the new DHS Strategy to Enhance International Supply Chain Security. This will then complete the first formal five year review and approval cycle mandated by MTSA.
- The Coast Guard intends to develop and deliver Underwater Terrorism Preparedness Plans to 12 additional ports.
- The Coast Guard is co-leading an effort with DHS to develop Adaptable Capability Packages of DHS-agencies specialized teams to respond and mitigate non-National Response Framework incidents. Testing of the concept continues with overall positive results.

GAO High-Risk Area - Protecting the Federal Government's Information Systems and the Nation's Critical Infrastructures

Summary of High-Risk Identification – As identified by GAO, protecting Federal computer systems and the systems that support critical infrastructures - referred to as cyber critical infrastructure protection - is a continuing concern. The continued risks to information systems include escalating and emerging threats such as phishing, spyware, and spam; the ease of obtaining and using hacking tools; the steady advance in the sophistication of attack technology; and the emergence of new and more destructive attacks.

GAO notes that as the focal point for Federal efforts to protect the Nation's critical infrastructures, DHS and its National Cyber Security Division have key cybersecurity responsibilities and claims that DHS has not yet completely fulfilled any of its key responsibilities. As an example, GAO asserts that DHS has not yet developed national cyber threat and vulnerability assessments or public/private recovery plans for cybersecurity. Per GAO, progress has been impeded by several challenges, including the reluctance of many in the private sector to share information with DHS, and a lack of departmental organizational stability and leadership needed to gain the trust of other stakeholders in the cybersecurity world.

2007 Accomplishments

DHS' National Cyber Security Division (NCSD), within the Office of Cyber Security and Communications (CS&C), continues to make progress developing and enhancing cyber analysis, watch and warning, and collaboration with the private sector:

- NCSD's U.S. Computer Emergency Readiness Team (US-CERT) provides a 24 hour, 7-day a week watch center to conduct daily analysis and situational monitoring to provide information on incidents and other events, as they are detected, to raise awareness and
- understanding of the current operating environment. The timely detection and analysis of cyber attacks helps to assess operational risk and mitigate the impact to our Nation's critical infrastructure.
- US-CERT's Einstein program enables the rapid detection of current and pending cyber attacks affecting agencies and provides Federal agencies with early incident detection. The information gathered by Einstein is used to provide actionable and timely alerts and reporting regarding current and impending cyber attacks, as well as indications and warnings of actual and potential intrusions to Federal Government computer security teams.
- US-CERT produces products that increase awareness among public and private sector stakeholders, including critical infrastructure owners and operators. This near real-time data collection and information sharing reduces cyber infrastructure vulnerabilities. US-CERT notifies public and private partners through a variety of products that encompass the National Cyber Alert System (NCAS). US-CERT established a vulnerability remediation process and the NCAS to collect, mitigate, and disseminate vulnerability information. NCAS is America's first cohesive national cyber security system for identifying, analyzing, and prioritizing emerging vulnerabilities and threats. NCAS delivers targeted, timely, and actionable information for technical and non-technical

audiences to enhance security. NCAS reports are made available through the NCAS, Information Sharing and Analysis Centers (ISACs), and on the US-CERT public website.

- Specifically for critical infrastructures, US-CERT produces Critical Infrastructure Information Notices (CIIN). Similar to the Federal Information Notice (FIN) provided to Federal agencies, the products are intended to provide information about a cyber security incident and make recommendations for avoiding or mitigating risks. The CIIN is specifically written to notify private sector organizations and Federal agencies involved with the protection of critical infrastructure.
- US-CERT relies on its collaboration with a variety of stakeholders and is working to formalize processes and procedures for collaboration with the private sector. US-CERT developed a draft concept of operations (CONOPs) for Private Industry Cyber Security Incident Handling that addresses information sharing, communication, and coordination with the private sector, including the ISACs. The CONOPs, which will be finalized in the near future, addresses sharing activities and coordination efforts with the private sector for cyber incidents, including Internet disruption.

In addition, CS&C:

- Drafted US-CERT Private Sector Concept of Operations (CONOPS).
  - Implemented US-CERT CONOPS across the Federal Government; the Office of Management and Budget (OMB) determined the US-CERT CONOPS to be a government regulation for Federal Government agencies within OMB.
  - Updated and implemented US-CERT CONOPS with the White House Policy Coordination Committee to define Personal Identifiable Information (PII) reporting requirements.
  - Refined Standard Operating Procedures (SOPs) to be consistent with US-CERT CONOPS.
- Standardized incident reporting across the government utilizing US-CERT's new incident tracking mechanism.
- Established an integrated joint operations center comprised of public and private sector members consisting of IT and communications organizations.
- Co-located US-CERT and National Coordinating Center for Telecommunications watch operations to facilitate the sharing of critical cyber and communications information.
- Engaged with the Partnership for Critical Infrastructure Security (PCIS) and Information and Analysis Center (ISAC) Council to develop a CONOPS and associated plans for coordinated watch and warning and incident response.
- Consistent with the NIPP Risk Management Framework, identified, assessed, and prioritized risks to the IT and Communications infrastructure, by analyzing threat, vulnerability, and consequence information.
- Continued to expand the National Vulnerability Database (NVD) to help establish a national baseline of specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance).
- Provided outreach to the seventeen CI-KR sector operators; this provided situational awareness for analysis across the Federal Government, critical infrastructure, and the

private sector, and enabled the US-CERT Analysis Program to correlate significant cyber incidents.

Remaining Plans

The Department has also held, and will continue to hold, exercises as mechanisms to identify ways to improve and promote public and private sector interaction toward enhancing situational awareness that supports decision making, communicating appropriate information to key stakeholder and the public, and planning and implementing response and recovery activities:

- NCSD is actively planning its second large-scale national cyber exercise, Cyber Storm II, which will be held in 2008. The exercise will build on Cyber Storm I, which enhanced DHS' relationship with private sector participants and helped to establish trust between the public and private sectors for future information sharing efforts. Cyber Storm II is being planned in close coordination with its stakeholders and participants. The exercise will feature a cyber-focused scenario that will escalate to the level of a cyber incident requiring a coordinated Federal response. Cyber Storm II is part of DHS' ongoing risk-based management effort to use exercises to enhance government and private sector response to a cyber incident, promote public awareness, and reduce cyber risk within all levels of government and the private sector.
- Cyber Storm II will also provide an opportunity to exercise new government and private sector concepts and processes developed since Cyber Storm I, such as Concepts of Operations and Standard Operating Procedures. The scenario will utilize coordinated cyber and physical attacks on critical infrastructures within selected sectors to meet a specific political and economic agenda (these cyber attacks will be simulated and will not impact any live networks). Participation will include Federal, State, local, and
- international governments, as well as private sector players from multiple critical infrastructure sectors. These types of exercises enable DHS to maintain and strengthen cross-sector, inter-governmental and international relationships, enhance processes and communications linkages, and ensure continued improvement to cyber security procedures and processes. Exercises also promote information sharing among participants and build relationships for future collaboration.

In addition, CS&C will:

- Increase manpower for 24/7 US-CERT Operations Center to provide the capability for in-depth incident tracking, detection, and mitigation.
- Continue to respond with a coordinated national system to major cyber and communications disruptions to restore essential communications.
- Continue to establish an integrated joint operations center comprised of public and private sector members consisting of IT and communications organizations.
- Continue to work with international partnerships to enable security partners to work together to promote secure, resilient IT and communications infrastructure.
- Continue to identify, assess, and prioritize risks to the IT and Communications infrastructure by analyzing threat, vulnerability, and consequence information.

- Continue to expand the National Vulnerability Database (NVD) to help establish a national baseline of specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance).

GAO High-Risk Area - Implementing and Transforming the Department of Homeland Security

Summary of High-Risk Identification: GAO designated implementing and transforming DHS as high-risk in 2003 because DHS had to transform and integrate 22 agencies – several with existing program and management challenges – into one department, and failure to effectively address its challenges could have serious consequences for homeland security.

Managing the transformation of an organization of the size and complexity of DHS requires comprehensive planning and integration of key management functions that will likely span a number of years. DHS has made progress in these areas but additional work is required to ensure sustainable success (GAO-07-833T).

2007 Accomplishments

- Outlined and monitored financial material weakness corrective actions and built internal control management assertions in the Internal Control Over Financial Reporting (ICOFR) Playbook.
- Increased IT system availability and disaster recovery capability with 24/7 operational support and infrastructure security in preparation for national incidents or disasters by initiating the migration of legacy data centers to two DHS Data Centers.
- Implemented a strategy to enhance information sharing by improving workflow, document management, and business processes to increase user satisfaction by 40 percent, decrease cost by 15 percent, and reduce production time by 25 percent.
- Improved interoperable facility and system access for employees by issuing a single, secure, tamper-proof smartcard; the first card was issued prior to the October 27, 2006 deadline.
- Increased procurement operational and strategic sourcing effectiveness by implementing a central DHS-wide Program Management Support Office.
- Implemented a strategy to improve the hiring and retention of talent needed to achieve DHS' mission by focusing on five key priorities in the FY 2007-2008 Human Capital Operational Plan.
- Improved leadership preparation by developing and implementing a Department-wide senior executive service development program.
- Streamlined training delivery and opportunities for employees through a new enterprise Learning Management System (currently available to DHS Headquarters, Transportation Security Agency (TSA), and other Component employees).
- Designed a consolidated DHS Headquarters facility that will co-locate disparate national capital regional offices. The design completes phase one of the consolidation plan.

Remaining Plans

- Review alignment of department programs and projects to updated mission goals and work to improve consistent and transparent method to measure the *status* and *progress* of defined performance expectations for projects and programs.
- Develop action plans to correct and monitor internal control weaknesses and compliance using GAO guidance such as "*Standards for Internal Control in the Federal Government*."
- Improve performance measures with the assistance of department-wide program analyst and evaluation teams.
- Issue Integrated Planning Guidance informed by threat and vulnerability assessments for budget planning cycles.
- Create technology initiatives that provide real-time connectivity between forward incident commanders and Joint Field Office communication platforms.
- Ensure more effective procurement practices across Department contracting offices through strategic sourcing and supplier management.

GAO High-Risk Area – Establishing Appropriate and Effective Information-Sharing Mechanisms to Improve Homeland Security

Summary of High-Risk Identification: As stated in the 2007 GAO high-risk report update, the Federal Government still faces formidable challenges in analyzing and disseminating key information among Federal, State, local, and private partners in a timely, accurate, and useful manner. Since September 11, 2001, multiple Federal agencies have been assigned key roles for improving the sharing of information critical to homeland protection to address a major vulnerability exposed by the attacks, and this important function has received increasing attention. However, the underlying conditions that led to the designation continue and more needs to be done to address these problems and the obstacles that hinder information sharing.

The Federal Government still has not implemented the government-wide policies and processes that the 9/11 Commission recommended and that Congress mandated. Completing the information sharing environment is a complex task that will take multiple years and long-term administration and congressional support and oversight, and will pose cultural, operational, and technical challenges that will require a collaborated response.

Federal agencies are also focusing on improving sharing with States, localities, and the private sector - a critical step since they are our first line of defense against terrorists - but these efforts are not without challenges. DHS has implemented a program to protect sensitive information the private sector provides on security at critical infrastructure assets, such as nuclear and chemical facilities. However, users of the information network were confused and frustrated with the system and as a result do not use it regularly; and DHS has still not won all of the private sector's trust that the agency can adequately protect and effectively use the information that sector provides. These challenges will require longer-term actions to resolve.

However, the Department notes that implementation and initial manning of DHS' State and Local Fusion Centers (SLFC) over the last year has gone a long way toward improving the information sharing nexus between DHS and its partners. DHS' primary partners are State and local governments (including tribal and territorial) and the private sector. These entities collect information outside the boundaries of the Intelligence Community (IC). Simultaneously, they have information needs not always recognized by the traditional IC agencies. DHS was created, in part, to bridge this gap and develop fusion at the *national*, vice *federal*, level.

To meet their own all-threats, all-hazards information needs many states and larger cities have created fusion centers. Fusion centers represent the logical touch-points for DHS to harvest local information and to provide them with timely relevant information and intelligence derived from all sources and analysis.

The DHS support effort provides ***people and tools*** to the SLFCs to create a web of interconnected information nodes across the country that will ensure information is gathered from all relevant operations and is fused with information from the Homeland Security Stakeholder Community to enable SLFCs and DHS to produce accurate, timely, and actionable intelligence products and services in support of homeland security.

On June 7, 2006, the Office of Intelligence & Analysis (I&A) was designated as the Executive Agent to manage the DHS State and Local Fusion Center program. It has been codified by PL 110-53, the law implementing the recommendations of the 9/11 Commission. This law requires that DHS take a stronger, more constructive role to assist SLFCs.

The SLFC Program is a major initiative to engage all players, at all levels of government, in confronting threats to the Homeland. It is a key element of DHS' strategy to exchange information with State and local authorities. Our goal is to create analytic centers of excellence nationwide to develop and exchange information with the Federal Government.

2007 Accomplishments

- The Secretary of Homeland Security issued a DHS-wide policy on information sharing, *DHS Policy for Internal Information Exchange and Sharing*, which provides guidance for all departmental information sharing activities. To supplement this memorandum, additional policy guidance and an Information Sharing and Access Agreement (ISAA) Guidebook are being developed to assist Components in creating information sharing agreements.
- DHS has established and is operating a three-tiered governance structure for information sharing. At the executive level, the Information Sharing Governance Board (ISGB) meets quarterly to decide department-wide information sharing issues. At the management level, the Information Sharing Coordinating Council, comprised of representatives from all DHS Components and offices, meets semi-monthly to bring information sharing issues to the table and to formulate recommendations for the ISGB. At the execution level, the Shared Mission Communities and Integrated Project Teams meet regularly to develop solutions for information sharing issues.

- Through the governance structure, a Law Enforcement SMC was established, which represents the first time that DHS law enforcement components have come together to discuss their mutual needs for information sharing. The LE-SMC is in the process of finalizing a DHS Law Enforcement Information Sharing Strategy.
- In response to direction from the ISGB, DHS is finalizing a department-wide Concept of Operations (CONOPS) for how components of the Department will interact with State and local fusion centers to ensure consistency and continuity.
- DHS created a department-wide metric for information sharing as part of the Department's Performance Plan that will examine compliance against the DHS policy on information sharing.
- The Secretary added a goal on information sharing to the Secretarial Priorities. The Department will measure its progress against this goal on a monthly basis.
- Last year Intelligence & Analysis (I&A) started the State and Local Fusion Program to deploy intelligence officers to fusion centers. I&A is deploying people and tools to build a national fusion center network.
- Recognition of I&A's efforts by Congress in the 9/11 Implementation law will help I&A build and sustain the Program.
    - Currently I&A has 19 intelligence officers deployed nationwide.
    - The Secretary has committed to 35 deployed officers by the end of FY 2008.
- Homeland Secure Data Network (HSDN), DHS' SECRET-level data network, is in 18 centers and will be doubled by the end of FY 2008.
    - I&A is building an analytic training program – equivalent to what it has for its own officers – for the state and local analysts in fusion centers.
    - Privacy and civil rights training is being developed and will be delivered as well.
- I&A's officers in the fusion centers help to develop the human network that creates true information sharing across the country. They are the link to I&A, DHS, and the Intelligence Community from our State and local partners.
- I&A is focused on supporting the SLFCs as the centers of gravity in each state. I&A:
    - provides the national threat perspective, warning information, and responses to requests to information,
    - writes products for, and with, state and local customers,
    - collaborates in researching topics with subject matter experts in SLFCs,
    - hosts analytic exchange conferences,
    - provides daily intelligence support,
    - posts and disseminates raw and finished intelligence products on HSIN State and Local unclassified portal and HSDN (classified network), and
    - supports development of Homeland Intelligence Reports (HIRs) from state- and local-origin information to provide to the Intelligence Community.
- Current Department of Defense (DoD) policy prevents us from giving access to the intelligence on SIPRNET via HSDN to our State and local partners. We have been working with DoD for the past year to change that policy and ensure that our investment in providing HSDN access to State and locals will be as fruitful as possible, so that we can live up to our "responsibility to provide" federal information to these partners.

Remaining Plans

- In the area of SLFCs, the key to harvesting the value from them is in tailoring DHS' support offering to meet their specific needs. This process begins with an assessment of the SLFC by a team of staff officers. The result is a set of recommendations on staffing and services that will deliver value to both DHS and the Fusion Center. Assessments have been conducted at 27 Fusion Centers across the country. Assessments will be done at more centers in FY 2008.
- Based on the results of the SLFC assessments and other factors, DHS has deployed intelligence officers to State Fusion Centers in Maryland, Georgia, Louisiana, Arizona, New York, Virginia, Illinois, Florida, California, Ohio, New Jersey, Massachusetts, Connecticut, and Washington State as well as to major city or regional centers in New York City, Los Angeles, and Dallas. The intent is to deploy officers to several more locations this year. As resources permit, DHS plans to have officers in as many as 35 sites by the end of fiscal year 2008.
- All SLFCs will soon have access to the HSDN, a SECRET collateral capability. Every SLFC will have an HSDN webpage to post State- and local-origin products making them available to other SLFCs and the Intelligence Community. These systems will create the information sharing environment necessary to enable information flow among the DHS intelligence and operational communities and the States.

GAO High-Risk Area – National Flood Insurance

Summary of High-Risk Identification – GAO placed the National Flood Insurance Program (NFIP) on its high-risk list in March 2006 because the NFIP will unlikely generate sufficient revenues to repay the billions borrowed from the Department of the Treasury to cover flood claims from the 2005 hurricanes. And it is unlikely that NFIP—a key component of the Federal Government's efforts to minimize the damage and financial impact of floods—could cover catastrophic losses in future years. Estimated claims for Hurricanes Katrina, Rita, and Wilma far surpass the total claims paid in the 38-year history of the NFIP. The insufficient revenues highlight structural weaknesses in how the program is funded.

The NFIP, by design, is not actuarially sound. Total collected premiums will unlikely be sufficient to pay all expected flood losses over time. In addition, the program is not structured to build loss reserves like a typical commercial insurance company, and it does not build and hold capital. Instead, it generally pays claims and expenses out of current premium income. When it has insufficient income to pay claims, the NFIP has authority to borrow from Treasury. It is highly unlikely that the NFIP, as currently funded, could generate revenues to repay Treasury, particularly if future hurricanes result in loss levels greater than the average historical loss levels.

2007 Accomplishments

- Improved NFIP delivery by: (a) distributing the *NFIP Summary of Coverage* and the *Flood Insurance Claims Handbook* to policyholders; (b) issuing informative supplemental policy coverage forms with new and renewed flood insurance policies; (c) providing Acknowledgement Forms to flood insurance policy purchasers; (d)

implementing important agent-training initiatives, (e) adopting a flood insurance claims appeals rule, and (f) carrying out initiatives that address repetitive loss properties.

- In FYs 2006 and 2007, FEMA transferred $40 million from the National Flood Insurance Fund to mitigate severe repetitive loss properties. The FY 2008 President's Budget requested an additional $80 million for SRL.
- The Severe Repetitive Loss (SRL) Interim Rule was published on October 31, 2007 at 72 FR 61720. After the regulations go into effect on December 3, 2007, FEMA will provide guidance to potential applicants, and will begin awarding funds.
- Greatly increased the number of agents who are trained to sell flood insurance.
- The Repetitive Flood Claims Program distributed a total of $19.8 million in FY 2006 and 2007 to help communities remove more than 80 buildings from floodplains.
- The Flood Mitigation Assistance Program committed $31 million to States for various floodplain management projects and plans. These programs, combined with flood insurance and other mitigation activities are important elements of a systematic effort to eliminate the flood-rebuild-flood scenario.
- Through the delivery of the Floodplain Management programs in FY 2007 and FY 2008, FEMA continues to lead a national effort to:
    - Identify and improve the understanding of communities' flood hazards and their risks by providing flood hazard maps.
    - Develop and improve techniques and planning processes which mitigate those flood risks.
    - Provide technical assistance and an environment at the State and local levels that is conducive to applying those techniques and processes.
    - Provide financial assistance to states to support State NFIP implementation and compliance activities.
    - Support development of incentives and disincentives that make application of those techniques and processes a social, political, and/or economic priority.

Remaining Plans

- Issue SRL program implementation plans and guidance in December 2007, and solicit and award grant applications. This initial implementation year will include FY 2006, 2007 and 2008 funding.
- FEMA will continue efforts to streamline the grant award process for all hazard mitigation assistance program grants, including Flood Mitigation Assistance (FMA), SRL and Repetitive Flood Claims (RFC). Guidance will be issued early in the fiscal year so as to open and close the application period earlier. In FY 2008, FEMA expects to expand the mitigation options available under the RFC program to include property acquisitions, elevations, dry flood-proofing and minor localized flood control projects to achieve the greatest savings to the fund in the shortest time. In FY 2008, approximately 15 awards to communities for 35 to 40 properties are expected. Efforts to engage partners and coordinate implementation of the FMA and RFC programs with the expanded SRL program will be continued.

Appendix A
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Executive Secretariat
Chief of Staff
Deputy Chief of Staff
General Counsel
Under Secretary Management
Assistant Secretary for Public Affairs
Assistant Secretary for Policy
Assistant Secretary for Legislative Affairs
Chief Financial Officer
Chief Information Officer
Chief Security Officer
Chief Privacy Officer
DHS OIG/GAO Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS' OIG Program Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- **Call our Hotline at 1-800-323-8603;**
- **Fax the complaint directly to us at (202) 254-4292;**
- **Email us at DHSOIGHOTLINE@dhs.gov; or**
- **Write to us at:**
  DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations - Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.