Office of Inspector General

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

December 4, 2006

MEMORANDUM FOR: The Honorable Michael Chertoff
Secretary

FROM: Richard L. Skinner
Inspector General

SUBJECT: *Major Management Challenges Facing the Department of Homeland Security*

Attached for your information is our annual report, *Major Management Challenges Facing the Department of Homeland Security*. The report was included in DHS FY 2006 Performance and Accountability Report. The report, including the department's comments in their entirety, will be posted on our public website.

Should you have any questions, please call me, or your staff may contact David M. Zavada, Assistant Inspector General for Audits, at (202) 254-4100.

Attachment

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Major Management Challenges Facing the Department of Homeland Security

(Excerpts from the FY 2006 DHS Performance and Accountability Report)

OIG-07-12

December 2006

Office of Inspector General

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

December 4, 2006

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 2006 Performance and Accountability 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

Homeland Security

December 4, 2006

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*, 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's action.

CATASTROPHIC DISASTER RESPONSE AND RECOVERY

DHS's failures after Hurricane Katrina ravaged the Gulf Coast on August 29, 2005, illuminated longstanding problems within the Federal Emergency Management Agency (FEMA). Many of the problems have existed for years, but never received the attention needed to fix them because FEMA had never before dealt with such a devastating disaster. Some estimate that the total federal response and recovery cost could reach $200 billion or more. FEMA has shortcomings in managing assistance and housing for evacuees, information systems, contracts and grants, and implementing the National

Flood Insurance Program.[1] We are planning additional work to assess FEMA's readiness to respond to future catastrophic disasters.

DHS and FEMA have learned many lessons from Katrina and have taken steps to improve their ability to respond to catastrophic disasters. For example, DHS and its federal partners revised the Catastrophic Incident Supplement to the National Response Plan to establish a better-coordinated strategy for a federal response to a catastrophic disaster. FEMA is working to improve its ability to house large numbers of evacuees and its logistics capability to supply commodities to disaster victims more quickly. But, it must implement catastrophic housing and logistics plans that are tested and exercised.

Possibly the largest problem FEMA faced in the aftermath of Katrina was assisting, sheltering, and housing evacuees. Never before had so many people been displaced for an extended period of time. FEMA's existing programs were inadequate to handle the problem, and FEMA's efforts to house victims in travel trailers and mobile homes were not well managed. Also, the number of victims overwhelmed FEMA's system for verifying their identities and providing individual assistance payments. The result of FEMA's efforts to speed up the process resulted in widespread fraud. In February 2006, we reported on weaknesses in FEMA's registration intake controls and recommended actions to improve them.[2] FEMA has improved its intake process and the system's capacity, but the changes are untested and may not be sufficient to address existing deficiencies. We are reviewing these problems and will help FEMA find solutions so it will be better prepared for the next catastrophic disaster or even multiple catastrophic disasters.

We have focused substantial work on FEMA contracting and have identified numerous problems. Our work indicates that FEMA was not well prepared to provide the kind of acquisition support needed for a catastrophic disaster. FEMA's overall response efforts suffered from (1) inadequate acquisition planning and preparation for many crucial needs, (2) lack of clearly communicated acquisition responsibilities between FEMA, other federal agencies, and state and local governments, and (3) insufficient numbers of acquisition personnel to manage and oversee contracts. In February 2006, we reported that FEMA purchased mobile homes without having a plan for how the homes would be used. As a result, FEMA now has thousands of surplus mobile homes.[3] In September 2006, we reported that FEMA spent $7 million renovating a facility to house evacuees. Because there was inadequate planning, the facility was never needed. As a result, the facility was underutilized.[4] FEMA has already made improvements; such as increasing the number of standby contracts in place and ready to be executed when disaster strikes. Also, DHS created a Disaster Response/Recovery Internal Control

[1] DHS-OIG, *Performance Review of FEMA's Disaster Management Activities in Response to Hurricane Katrina*, OIG-06-32, March 2006.
[2] DHS-OIG, *Strengthening Registration Intake Controls*, OIG GC-HQ-06-10.
[3] DHS-OIG, *Mobile Homes and Modular Homes at Hope and Red River*, OIG GC-HQ-06-12.
[4] DHS-OIG, *Starship Facility Renovation Project*, OIG GC-HQ-06-52.

Oversight Board to address many of the problems. We will soon conduct a review of FEMA's overall acquisition management structure to identify additional improvements that FEMA can make to be prepared better for the next catastrophic disaster. We will review organizational alignments and leadership, policies and procedures, FEMA's acquisition workforce, and its information management. We are also reviewing FEMA's system for accounting for property it has purchased for disasters.

Hurricane Katrina highlighted the need for data sharing among federal agencies following a catastrophic disaster. We see a need for data sharing in three areas. Real-time data exchange among agencies would help verify eligibility of applicants for disaster assistance and simplify the application process for victims. Direct access to FEMA data by law enforcement agencies would help identify and track convicted sex offenders and suspected felons, and help locate missing children. Computer data matching would help to prevent duplicative payments and identify fraud. FEMA is moving in the right directions on these issues. For example, FEMA has granted direct access to its data to the Hurricane Katrina Fraud Task Force for the purpose of investigating fraud. However, progress is slow and much remains to be done. FEMA and the federal community are not ready to meet the data sharing requirements of the next catastrophic disaster.

FEMA issued approximately 2,700 mission assignments totaling about $8.7 billion to federal agencies to help with response to Hurricane Katrina. FEMA historically has had significant problems issuing, tracking, monitoring, and closing mission assignments. FEMA guidance on the missions is often vague, and agencies' accounting practices vary significantly, causing problems with reconciling agencies' records to FEMA records. FEMA has developed a number of new pre-defined mission assignments to streamline some of the initial recurring response activities. In addition, FEMA's Disaster Finance Center is working to find a consensus among other Federal agencies on appropriate supporting documentation for billings. We are conducting a review of mission assignments to DHS agencies and other Inspectors General are reviewing mission assignments to their respective agencies.

We are also planning a review of FEMA's National Flood Insurance Program (NFIP). Floods are among the most frequent and costly of all natural disasters and have great impact in terms of economic and human losses each year. FEMA is now faced with NFIP issues ranging from outdated flood maps to the question of whether damages are the result of flooding from storm surge or hurricane winds. Many NFIP related questions need to be addressed before the next catastrophic flood.

ACQUISITION AND CONTRACT MANAGEMENT

DHS must have an acquisition management infrastructure in place that allows it to oversee effectively the complex and large dollar procurements critically important to achieving DHS's mission. Acquisition management 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.

We identified significant risks and vulnerabilities that might threaten the integrity of those operations. In general, DHS needs more comprehensive acquisition guidance and oversight.[5] Other vulnerabilities fall into three general categories: adherence to ethical conduct, program management, and procurement management.

- In the area of ethical conduct, senior program managers and procurement officials would benefit from expanded training and guidance on their procurement ethics responsibilities. DHS's many partnership arrangements with the private sector suggest that the minimal initial and annual government ethics training DHS requires may be insufficient. The Office of the Chief Procurement Officer (OCPO) is working with DHS ethics officials to develop effective online training for procurement executives and operational specialists. This training will expand on the initial training and provide relevant ethics scenarios. The training will also provide a mechanism for procurement executives to request additional information and assistance as ethics issues arise. In addition, OCPO has piloted acquisition ethics training targeted towards senior management. This pilot has been presented to all heads of contracting activities and selected senior Immigration and Customs Enforcement (ICE) personnel.

- Effective program management is essential to obtaining the right equipment and systems to accomplish the DHS mission. Complex and high dollar contracts require multiple program managers often with varying types of expertise. Several DHS procurements have encountered problems because contract technical and performance requirements were not well defined. DHS needs more certified program managers; comprehensive department-wide standards for program management; a strengthened investment review board process to provide greater independent analysis and review; better defined technical requirements; and more balance among schedule, cost, and performance when expediting contracts. OCPO recently established a program management advisory board, established standards for certifying program managers, and promoted program management training opportunities.

- In their transition into DHS, seven agencies retained their procurement functions, including the United States Coast Guard (USCG), FEMA, and the Transportation Security Administration (TSA). The expertise and capability of the seven procurement offices mirrors the expertise and capability they had before creation of DHS, with staff size that ranged from 21 to 346 procurement personnel. DHS established an eighth acquisition office, the Office of Procurement Operations (OPO),

[5] DHS-OIG, *Department of Homeland Security's Procurement and Program Management Operations*, OIG-05-53, September 2005.

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

In addition to awarding contracts, OCPO helps DHS components adhere to standards of conduct and federal acquisition regulations in awarding and administering contracts. This oversight role involves developing department-wide policies and procedures and enforcing those policies and procedures. Both our office and GAO have reported that the OCPO needs more staff and authority to carry out its general oversight responsibilities. GAO recommended that DHS provide OCPO with sufficient resources and enforcement authority to enable effective department-wide oversight of acquisition policies and procedures. We made a similar recommendation.

During FY 2006, the Under Secretary for Management established policies for acquisition oversight and directed each of the nine heads of contracting activities to measure and manage their acquisition organizations.[6] Also, the number of oversight specialists in the Acquisition Oversight Division of OCPO is authorized to expand to nine during FY 2007. OCPO is working to hire the additional staff. OCPO has undertaken an outreach program to involve DHS component staff to manage effectively and assist in acquisition oversight.

We have conducted audits and reviews of individual DHS contracts, such as TSA's screener recruiting and TSA's information technology services. Common themes and risks emerged from these audits, primarily the dominant influence of expediency, poorly defined requirements, and inadequate oversight that contributed to ineffective or inefficient results and increased costs.

The urgency and complexity of DHS's mission will continue to demand rapid pursuit of major investment programs. While DHS continues to build its acquisition management capabilities in the component agencies and on the department-wide level, the business of DHS goes on and major procurements continue to move. On November 2, 2005, DHS announced a multi-year strategy to secure America's borders and reduce illegal immigration, called the Secure Border Initiative (SBI). The SBI procurement presents a considerable acquisition risk because of its size and scope. We see risks and vulnerabilities similar to those identified in previous OIG audits and reviews.

---

[6] DHS, *Acquisition Oversight Program*, Management Directive System MD number 0784, December 19, 2005.

USCG has also encountered a number of challenges in executing its Deepwater Acquisition program despite the expenditure of more than $3 billion over four years. This is particularly true within the Deepwater surface and air domains. For example, the 110-foot patrol boat conversion project was curtailed at eight cutters due to design, construction, performance, and cost concerns. Further, strict operational restrictions have been imposed on these cutters until additional structural analyses can be completed. In response to these challenges, USCG accelerated plans to design, construct, and deploy the composite Fast Response Cutter (FRC) by more than 10 years as a replacement for the 110-foot patrol boat. However, an independent analysis confirmed that the FRC design is outside patrol boat design parameters, i.e., too heavy, too overpowered, and not streamlined enough to reduce resistance. These concerns led to USCG's April 2006 decision to suspend work on the FRC until these issues could be resolved or an alternative commercial off-the-shelf design identified. In the Deepwater air domain, the HH-65C helicopter[7] and unmanned aerial vehicle (VUAV) acquisitions have encountered schedule delays and cost increases. These Deepwater design, construction, performance, scheduling, and cost issues are expected to present significant challenges to USCG's Deepwater Program during FY 2007.

Providing Accurate and Timely Procurement Reporting

In July 2006, we reported on the challenges that DHS faces in planning, monitoring, and funding efforts to ensure the accurate and timely reporting of procurement actions to interested stakeholders.[8] The Executive Branch, the Congress, and the public rely upon such procurement information to determine the level of effort related to specific projects and also to identify the proportion of government contracts that are awarded to small businesses. Currently, however, DHS has several different contract writing systems that do not automatically interface with its Federal Procurement Data Systems - Next Generation (FPDS-NG) – a government-wide procurement reporting system accessible by the public. Some of the systems may need to be replaced. Additionally, not all DHS procurements are entered into FPDS-NG. For example, grants, mission assignments, and purchase card data may not be entered into FPDS-NG, resulting in an understatement of DHS's procurement activities.

DHS has undertaken a number of initiatives to improve its reporting on procurement actions. These initiatives include interfacing the various DHS contract-writing systems with FPDS-NG and ensuring that all procurement information is entered into FPDS-NG immediately following contract award. Such initiatives will not only enable real-time reporting of DHS procurement actions; they also will allow DHS to rely on General

[7] DHS-OIG, *Re-Engining of the HH-65 Helicopter, United States Coast Guard*, OIG-04-50, September 2004.
[8] DHS-OIG, *DHS' Management of Automated Procurement Systems Needs Improvement*, OIG-06-46, July 2006.

Services Administration databases to help eliminate contract awards to ineligible vendors. OCPO has worked with each of the DHS components to improve the accuracy, completeness, and timeliness of FPDS-NG data entry. DHS's planned deployment of a single contract writing software system should reduce duplicate data entry for each contract action. DHS is developing routine reporting for non-FPDS-NG instruments.

GRANTS MANAGEMENT

Managing the multitude of grant programs within DHS poses a significant challenge. Further, the grant programs of other federal agencies that assist states and local governments in improving their abilities to prepare for, respond to, and recover from acts of terrorism or natural disasters compound this challenge. Congress continues to authorize and appropriate funding for individual grant programs within and outside of DHS for similar, if not identical, purposes. In total, DHS manages over 80 disaster and non-disaster grant programs. For disaster response and recovery efforts, we have identified 36 federal assistance programs that have the potential for duplicating DHS grant programs. DHS must do more to coordinate and manage grants that are stove-piped for specific, but often related purposes to ensure that they are contributing to our highest national preparedness and disaster recovery goals, rather than duplicating one another and being wasted on low-priority capabilities.

Disaster grant awards will be substantially larger than usual with the over $60 billion that Congress appropriated in late FY 2005 for disaster response and recovery efforts related to Hurricanes Katrina, Wilma, and Rita. In the Gulf Coast states affected by these hurricanes, numerous federal grants from different agencies and components of DHS are going to state and local governments, private organizations, and individuals for response and recovery from the recent hurricanes as well as for the next disaster or terrorist attack. We are currently reviewing disaster grant activities throughout the Gulf Coast and will continue to give special emphasis to Gulf Coast disaster response and recovery grant spending.

In FY 2005, DHS expected to award approximately $4.6 billion of non-disaster grants. We are reviewing individual state's management of first responder grants and the effectiveness of DHS's system for collecting data on state and local governments' risk, vulnerability, and needs assessments. Our audits have reported on the states' inability to manage effectively and monitor these funds and to demonstrate and measure improvements in domestic security. Our reports also pointed out the need for DHS to monitor the preparedness of state and local governments, grant expenditures, and grantee adherence to the financial terms and conditions of the awards.[9]

---

[9] DHS-OIG, *The State of Indiana's Management of State Homeland Security Grants Awarded During Fiscal Years 2002 and 2003,* OIG-06-19, December 2005; DHS-OIG, *The Commonwealth of Virginia's Management of State Homeland Security Grants Awarded During Fiscal Years 2002 and 2003,* OIG-06-45, July 2006.

DHS faces a challenge in addressing its responsibility to become an efficient and effective grants manager. For example, while the Office of Grants and Training is tasked with financial and programmatic monitoring and oversight for first responder grants, the Office of Justice Programs with the Department of Justice does the accounting for these grants. Given the billions of dollars appropriated annually for disaster and non-disaster grant programs, DHS needs to ensure that grants management internal controls are in place and adhered to, and that grants are sufficiently monitored to achieve successful outcomes. DHS needs to ensure that, to the maximum extent possible, disaster and homeland security assistance go to those states, local governments, private organizations, or individuals eligible to receive such assistance and that grantees adhere to the terms and conditions of the grant awards. DHS needs to continue refining its risk-based approach to awarding first responder grants to ensure that areas and assets that represent the greatest vulnerability to the public are as secure as possible. It must incorporate sound risk management principles and methodologies to successfully prepare for, respond to, recover from, and mitigate acts of terrorism and natural disasters. DHS is planning a study to provide a single grants management system for all non-disaster related grants.

FINANCIAL MANAGEMENT

Financial management has been a major challenge for DHS since its creation in 2003. This year, DHS was again unable to obtain an opinion on its financial statements, and numerous material internal control weaknesses continued to be reported. KPMG, LLP, under contract with the OIG, issued a disclaimer of opinion on DHS's 2003, 2004, and 2005 financial statements.

DHS's material internal control weaknesses ranged from financial management oversight and reporting at the department level to controls surrounding the recording of individual account balances within DHS bureaus. These control weaknesses, due to their materiality, are impediments to obtaining a clean opinion and positive assurance over internal control at the department level.[10] Achieving these departmental goals is highly dependent upon internal control improvements at USCG, ICE, TSA, and the Office of the Chief Financial Officer (OCFO). Many of the Department's material weaknesses, to varying degrees, are attributable to USCG.

To move forward, DHS must develop a comprehensive financial management strategy that addresses organizational resources and capabilities, inconsistent and flawed business processes, and unreliable financial systems. An initial step in this process is to prepare well-developed and comprehensive corrective action plans to address known internal control weaknesses.

[10] DHS-OIG, *Independent Auditors' Report on DHS' FY 2005 Statements*, OIG-06-09, November 2005.

Over the past several months, we initiated a series of performance audits to assess the effectiveness of DHS's corrective action plans to address internal control weaknesses. Our objective in conducting these performance audits was to assess the thoroughness and completeness of both the overall corrective action plan process and individual plans developed to address specific weaknesses. The performance audits are intended to provide ongoing feedback to DHS as it is developing and implementing corrective action plans.

During FY 2006, we anticipated progress in addressing internal control deficiencies. DHS identified four areas where internal control weaknesses exist for improvement during the year. However, in our corrective action plan audits, we reported that a coordinated, department-wide effort to develop corrective action plans did not begin until the third quarter of 2006; and DHS is not expected to have a department-wide plan in place until the first quarter of FY 2007. At the component level, we identified well-developed corrective action plans at ICE, but little progress at USCG. During 2006, ICE began its corrective action plan process early and is showing signs of internal control improvements this year. Our audit reports provide recommendations for improvement at the department-wide and component levels.

INFORMATION TECHNOLOGY MANAGEMENT

Integrating the information technology (IT) systems, networks, and capabilities of the various legacy agencies to form a single infrastructure for effective communications and information exchange remains one of DHS's 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 also will remain untapped.

Department-wide IT Infrastructure

Creating an adequate disaster recovery capability for DHS's information systems is a major concern. DHS's IT infrastructure remains a collection of legacy networks, systems, and data centers. Several elements of this IT infrastructure do not have the ability to relocate to an alternate site that can be used if their primary facility suffers an

extended outage or becomes inaccessible. This inability to restore the functionality of DHS's 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.

However, due to a lack of sufficient funding and an operational program to support an enterprise-wide disaster recovery solution, DHS has been hindered in its efforts to provide an alternate processing facility. Specifically, DHS received a combined $85 million in FY 2005 and FY 2006 for the development, operations, and maintenance of 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's Chief Information Officer (CIO). Additionally, DHS has submitted a request for information for a second data center to supplement the 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. Ensuring that funds provided are spent effectively 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. Currently, DHS is in the process of addressing these communications requirements, which are critical for exchanging mission-critical information both within DHS and with outside stakeholders. Specifically, DHS is implementing a Multi-Protocol Label Switching (MPLS) technology on top of its asynchronous transfer mode and Frame Relay circuits. DHS hopes this MPLS infrastructure will allow the elimination of redundant firewalls and the replacement of hardware encryption devices with Internet Protocol Security encryption. At the same time, DHS is undertaking an ambitious effort to combine its various internal Security Operations Centers and Network Operations Centers, which help ensure that data communication within DHS, and with external stakeholders, is secure and functional. Coordinating these related communications upgrade efforts will require significant resources and oversight. 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's IT systems.

As we reported in September 2006, based upon its annual FISMA evaluation, excluding its intelligence systems, DHS achieved a significant milestone that will continue to help DHS move toward managing a successful information security program.[11] DHS implemented a department-wide remediation plan to certify and accredit all operational systems by the end of FY 2006. Completion of this task will eliminate a hurdle that prevented DHS from strengthening its security program. In addition, some of the issues that we identified in our FY 2005 FISMA report to assist DHS and its components in the implementation of its information assurance program have been addressed, such as developing a process to maintain a comprehensive inventory.

In addition to our FISMA evaluations, during the past year we conducted information security audits of DHS networks, databases, laptops, and Radio Frequency Identification systems. We also reviewed major programs, such as the Transportation Workers Identification Credential and U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT). Based on the results of these audits, as well as our FISMA evaluation, and despite several major improvements in DHS's information security program, DHS organizational components, through their Information Systems Security Managers, have not completely aligned their respective information security programs with DHS's overall policies, procedures, and practices. For example:

- All operational systems have not been adequately certified and accredited.
- All components' information security weaknesses are not included in a Plan of Action and Milestones report.
- Data in the enterprise management tool, Trusted Agent FISMA, is not complete or current.
- System contingency plans have not been tested for all systems.
- 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 establish comprehensive management authority over the information security

[11] DHS-OIG, *Evaluation of DHS' Information Security Program for Fiscal Year 2006*, OIG-06-62, September 2006.

program for DHS's intelligence systems. DHS must also ensure the confidentiality, integrity, and availability of vital intelligence information.

DHS Component IT Management

IT management at the subcomponent-level remains a major challenge, as demonstrated by our audits and subsequent reports on the IT programs and initiatives of selected DHS directorates and organizations. We repeatedly identified 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. Insufficient training and guidance to support IT users were typical.

For example, in September 2005, we reported that U.S. Citizenship and Immigration Services (USCIS) had not recognized the potential benefits of streamlining processes and leveraging IT to help meet its backlog reduction goals.[12] USCIS processes were primarily manual, paper-based, and duplicative, resulting in an ineffective use of resources to ship, store, and track immigration files. Adjudicators used multiple and non-integrated IT systems to perform their jobs, which reduced productivity and data integrity. IT software and hardware systems also were outdated and not well configured to meet user needs. Further, despite federal requirements, USCIS had not taken a focused approach to modernizing processes and systems to accomplish its citizenship and immigration services mission. We conducted a follow-up review of USCIS efforts to address our earlier report recommendations. While USCIS has made some progress by placing priority on business transformation, taking steps to centralize authority for IT personnel, initiating business process reengineering activities, and upgrading desktops and servers at key field locations, USCIS would benefit from improvements in centralizing IT operations and refining IT management practices. To be successful, USCIS also must ensure that its transformation strategy is clearly defined and managed.

Similarly, we reported in September 2005 that EP&R did not effectively manage IT to support incident response and recovery.[13] Specifically, although EP&R has made progress in IT planning, including development of FEMA's first IT strategic plan, the IT plan aligns with the agency's outdated strategic plan and does not reflect integration into DHS. As such, the IT plan provides no assurance that FEMA's systems will support accomplishment of department-wide missions and goals. Further, even though FEMA

[12] DHS-OIG, *USCIS Faces Challenges in Modernizing Information Technology*, OIG-05-41, September 2005.

[13] DHS-OIG, *Emergency Preparedness and Response Could Better Integrate Information Technology with Incident Response and Recovery*, OIG-05-36, September 2005. On October 1, 2005, EP&R was dismantled, with preparedness functions moved to the new Preparedness Directorate. FEMA, originally part of EP&R, became a separate DHS entity that reports directly to the Secretary and retained responsibility for consequence management after catastrophes, including response and recovery activities.

staff provided significant service during the 2004 hurricanes, additional guidance and training are needed to ensure that IT systems users have the knowledge and information required to perform their jobs in future response and recovery efforts. Moreover, FEMA's systems are not integrated and therefore do not effectively support information exchange among emergency managers. Inadequate IT requirements definition limits the agency's ability to identify alternatives to existing systems while insufficient test facilities hinder comprehensive evaluation of new systems prior to deployment. Our follow-up assessment of FEMA's efforts to upgrade its principal disaster management system shows 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.

Our reviews of major IT programs and initiatives of various components' management indicate similar problems. For example, in September 2005 we reported that FEMA could benefit from improvements to its six-year, $1.5 billion flood map modernization program to digitize flood maps used to identify flood zones and determine insurance requirements.[14] Although FEMA is making progress in the program, its Multi-Year Flood Hazard Plan does not effectively address user and funding needs. Current policies, agreements, and information sharing mechanisms do not effectively support coordination and cooperation among mapping stakeholders. Further, FEMA has made limited progress in developing a web-based mapping system due to unclear contractor expectations, underestimation of program scope and complexity, and poorly defined requirements, resulting in significant system acquisition delays and cost overruns. FEMA can strengthen its flood map modernization program by reviewing and revising its mapping plan, enhancing program guidance, increasing contractor oversight, and improving coordination with stakeholders. Clearly defining requirements and contractor expectations and maintaining standard methodologies for mapping system development also would help ensure program success.

In August 2006 we reported on improvements that USCG could make in its efforts to design and implement command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems as part of its estimated $20 billion Integrated Deepwater System (Deepwater) program.[15] Although USCG is making progress in the program, its limited influence over contractor decisions toward meeting Deepwater IT requirements and a lack of discipline in requirements change management processes provide little assurance that the requirements remain up-to-date or are effective in meeting program goals. In addition, certification and accreditation of Deepwater C4ISR equipment has been difficult to achieve and the contractor has not followed established IT testing procedures consistently, placing systems security and C4ISR operations at risk. Further, due to limited oversight, as well as unclear contract requirements, the agency cannot ensure that the contractor is making the best decisions

[14] DHS-OIG, *Challenges in FEMA's Flood Map Modernization Program*, OIG-05-44, September 2005.
[15] DHS-OIG, *Improvements Needed in the U.S. Coast Guard's Acquisition and Implementation of Deepwater Information Technology Systems*, OIG-06-55, August 2006.

toward accomplishing Deepwater IT goals. Insufficient C4ISR funding has restricted accomplishing the "system-of-systems" objectives that are fundamental to ensuring interoperability of Deepwater assets, such as ships and aircraft. Meeting the training and IT support needs of Deepwater C4ISR users also is key.

Information Sharing

The *Homeland Security Act of 2002*[16] makes coordination of homeland security communication with state and local government authorities, the private sector, and the public a key DHS responsibility. However, due to time pressures, DHS did not complete a number of the steps essential to effective planning and implementation of the Homeland Security Information Network (HSIN)—the sensitive, but unclassified, system it instituted to help carry out this mission. As such, effective sharing of the counter-terrorist and emergency management information critical to ensuring homeland security remains an ongoing challenge for DHS.

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.[17] DHS did not adequately evaluate each of its three major HSIN releases prior to their implementation. Further, DHS has not provided adequate user guidance, including clear information sharing processes, training, and reference materials. Without establishing a baseline and developing specific performance measures, DHS has no effective way to track or assess information sharing using HSIN. As a result of these system planning and implementation issues, HSIN is not meeting user needs and supporting state and local sharing of and situational awareness and counter-terrorist information. Therefore, potential users do not regularly use HSIN. Instead, they resort to pre-existing systems and telephone calls to share information, perpetuating the ad hoc, stove-piped information-sharing environment that HSIN was intended to correct. Resources, legislative constraints, privacy, and cultural challenges – often beyond the control of HSIN program management – also pose obstacles to HSIN's success.

On a broader scale, DHS is challenged with incorporating data mining into its overall strategy for sharing information to help detect and prevent terrorism. Data mining aids agents, investigators, and analysts in the discovery of patterns and relationships from vast quantities of data. *The Homeland Security Act* authorizes DHS to use data mining and 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.[18] For example, CBP performs matching to target high-risk cargo. The U.S. Secret Service automates the evaluation of counterfeit documents. TSA collects

[16] P.L. 107-296.
[17] DHS-OIG, *Homeland Security Information Network Could Support Information Sharing More Effectively*, OIG-06-38, June 2006.
[18] DHS-OIG, *Survey of DHS Data Mining Activities*, OIG-06-56, August 2006.

tactical information on suspicious activities. ICE detects and links anomalies indicative of criminal activity to discover relationships. However, without department-wide planning, coordination, and direction, the potential for integrating advanced data mining functionality and capabilities to address homeland security issues remains untapped.

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. The issuance of the National Infrastructure Protection Plan (NIPP) in June 2006 marked an unprecedented collaboration among federal, state, local, tribal, and private sector partners to establish the coordinated approach that will be used to establish national priorities, goals, and requirements for CI/KR protection so that federal funds and resources are applied in the most effective manner to reduce vulnerability, deter threats, and minimize consequences of attacks and other incidents. In addition, DHS has an oversight role in coordinating the protection of CI/KR, where 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.

The DHS FY 2007 Appropriations Act granted the Secretary of Homeland Security authority to issue regulations that establish risk-based performance standards for security of chemical facilities, and require vulnerability assessments and development and implementation of site security plans. However, the chemical sector is just one segment of an enormous and complex distribution of the nation's CI/KR. Reliance on the private sector as well as our federal partners to deter threats, mitigate vulnerabilities, or minimize the consequences associated with a terrorist attack or other incident creates a void in the assurance that all CI/KR are adequately protected. Combined with the uncertainty of the terrorist threat and other manmade or natural disasters make the effective implementation of protection efforts a great challenge.

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 management and resource allocation decision-making. As we reported in FY 2006, DHS is improving the development and quality of the NADB. DHS is also 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.

We are currently reviewing the Department's efforts to coordinate infrastructure protection activity within the food and agriculture sector, as well as implement buffer zone protection plans at critical infrastructure and key resource sites across the country. We will continue to monitor and review how DHS uses the NADB to support its risk management framework, how it coordinates infrastructure protection with other sectors, and how its pursuit of basic vulnerability assessment standards can help develop overarching departmental priorities.

BORDER SECURITY

One of DHS's 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.

During FY 2006, the White House and DHS announced a comprehensive multi-year plan to secure the borders and reduce illegal immigration, Secure Border Initiative (SBI). DHS created a program executive office within the policy directorate to oversee, plan, and coordinate implementation of SBI across DHS. This systems approach 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.[19] 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. 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.[20]

Maintaining a systems approach to addressing the challenge of securing our borders will be 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.

---

[19] DHS-OIG, *An Assessment of the Proposal to Merge Customs and Border Protection with Immigration and Customs Enforcement*, OIG-06-04, November 2005.
[20] DHS-OIG, *A Review of Remote Surveillance Technology Along U.S. Land Borders*, OIG-06-15, December 2005.

- 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 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 (ISIS) and the America's Shield Initiative (ASI). CBP awarded a 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. 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 has not properly defined, validated, and stabilized operational requirements and needs to do so quickly to avoid rework of the contractor's systems engineering and the attendant waste of resources and delay in implementation. Moreover, until the operational and contract requirements are firm, effective performance management and cost and schedule control is precluded. DHS also needs to move quickly to establish the organizational capacity to properly oversee, manage, and execute the program.

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's entry-exit system. It also coordinates the integration of two fingerprint systems: DHS's 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 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's 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

The *Aviation and Transportation Security Act* (ATSA),[21] enacted in response to the events of September 11, 2001, mandated that TSA hire and train thousands of screeners for the Nation's 438 commercial airports by November 19, 2002. As a result, TSA ultimately hired 45,000 screeners. 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. Four areas 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. Additionally, TSA has completed implementation of most of our recommendations in these areas and is continuing to work on the remaining recommendations. TSA has conducted several pilot programs at airports nationwide, such as the explosive trace portal (ETP) and the explosive detection scanner to facilitate enhanced screener performance.[22] We plan to evaluate TSA's performance in implementing these technologies.

TSA has been largely successful in its effort to implement the ATSA requirement that all checked bags be screened by explosives detection systems. However, improvements in

[21] P.L. 107-71.
[22] DHS-OIG, *Audit of Passenger and Baggage Screening Procedures at Domestic Airports*, OIG-04-37, September 2004, and DHS-OIG, *Follow-up Audit of Passenger and Baggage Screening Procedures at Domestic Airports (Unclassified Summary)*, OIG-05-16, March 2005.

screening passengers and their carry-on bags for explosives require additional work. For example, piloting of whole-body scanners – backscatter x-ray machines – at U.S. airports has been delayed until FY 2007. The only recent technology deployed to augment traditional passenger screening is ETP, which can detect explosive residue on passengers' bodies and clothing. Currently, TSA has deployed 94 ETPs at 37 different U.S. airports. However, on September 3, 2006, TSA's Chief Technology Officer said that some unanticipated ETP problems have temporarily halted deployment. TSA continues to solicit industry to submit technologies for evaluation and possible use in passenger and baggage screening. TSA recently issued requests for information soliciting manufacturers of commercially available whole-body imaging and advanced x-ray technologies to submit their technologies for evaluation.

Rail And Mass Transit

Passenger rail transit, bus, and ferry systems are extremely vulnerable to terrorist attack as evidenced by the attacks on passenger rail facilities in Madrid, London, and India. Surface transportation modes in the United States are inherently difficult to secure 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 (160,000 miles of interstate highway and other major roads included in approximately 3.8 million miles of roads nationwide, and more than 600,000 bridges and tunnels). About 500 bridges and tunnels have been identified as playing key economic or traffic handling roles, and, therefore, are potential terrorist targets. Although the FY 2007 DHS Appropriations Act provides $175 million for rail and public transit safety — an increase of $25 million over FY 2006 – the primary focus for transportation security and the accompanying resources continues to tilt heavily toward aviation security.

DHS has recently begun work in this area. Through the National Infrastructure Protection Plan (NIPP), DHS has established a forum and process to enhance coordination among federal, state, and local government entities for the communication and exchange of information. In one initiative to address vulnerabilities in surface transit modes, TSA led the formation of the Transportation Sector Government Coordination Council, which called for establishment of coordinating councils in each transportation mode. TSA leads a council, which includes the Department of Transportation (the Federal Transit Administration and the Federal Railroad Administration), created in March 2006 for transit and commuter and long-distance rail. This council's objective is to facilitate regional engagement and bring together federal, state, and local government partners and regional mass transit stakeholders in efforts to enhance security through consistent and effective security strategies and programs.

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 between federal, state, and local partners. DHS has made millions of dollars available through the Transportation Security Grant Program, Homeland Security

Grant Program, Highway Watch Program, Urban Area Security Initiative, and other funding methods. DHS also trains and deploys manpower for high-risk areas through the Multi-Modal Security Enhancement Teams and Surface Transportation Security Inspection Program Inspectors; and develops and tests new technologies, such as more effective chemical and explosive detection equipment, mobile security checkpoints, and video surveillance systems. Nevertheless, the task of prioritizing and securing surface transportation is daunting. While TSA, its government partners, and industry owners and operators have increased their vigilance, more robust information exchange, threat detection, and preparedness measures must be undertaken to ensure the security and resilience of the surface transportation system.

TRADE OPERATIONS AND SECURITY

Trade operations and security is primarily 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 or 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 (CSI), 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 the trade 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 developing a “smart” container that will provide extra protection or warning of tampering or intrusion. In support of its trade mission, CBP is undertaking an extensive and long-term effort to develop a new system, Automated Commercial Environment, to replace older, less effective, and less capable trade processing systems. This effort is not scheduled to be fully competed until 2011, and will cost more than $3.3 billion dollars.

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.[23] Ongoing reviews will provide further recommendations about the use of intelligence, the development of performance measures, cargo inspection, training, and control and inspection of high-risk sea containers.

USCG 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, USCG must balance the resources devoted to the performance of homeland and non-homeland security missions; improve the performance of its homeland security missions; maintain and re-capitalize USCG'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 USCG's homeland security missions grew steadily from FY 2001 through FY 2005,[24] USCG continues to experience difficulty meeting its performance goals for homeland security missions.[25]

[23] DHS-OIG, *Audit of Targeting Oceangoing Cargo Containers*, OIG-05-26, July 2005.
[24] FY 2001 through FY 2005.
[25] DHS-OIG, *Annual Review of Mission Performance, United States Coast Guard (FY 2005)*, OIG-06-50, July 2006.

MANAGEMENT'S RESPONSE TO THE OFFICE OF THE INSPECTOR GENERAL'S REPORT ON MAJOR MANAGEMENT CHALLENGES FACING THE DEPARTMENT OF HOMELAND SECURITY

The following provides specific responses to those issues raised by the Inspector General's (IG) statement on the top management challenges facing the Department.

The Department of Homeland Security has steadfastly worked to resolve the challenges identified in the Inspector General's FY 2005 report. Two challenges identified in that report are no longer reported as major management challenges; Consolidating the Department's components, and Human Capital Management. The reduction in the number of major challenge areas evidences the maturing of DHS as it continued its pursuit of organizational excellence; strategic goal number seven during FY 2006.

The Department will continue to address the unresolved management challenges identified in the Inspector General's report of 2005, many of which require more than twelve months to completely overcome. The following tables highlight the accomplishment of the Department during FY 2006, and some of the remaining plans to be completed in the future to overcome these challenges.

FY 2006 Challenge 1: Catastrophic Disaster Response and Recovery
FY 2005 Challenge 1: Disaster Response and Recovery The report raised concerns regarding weaknesses in FEMA information systems, the flood map modernization program, contract management, grants management, and the individual assistance program. In addition, since FEMA's programs are largely administered through grants and contracts, the circumstances created by Hurricanes Katrina and Rita provided an unprecedented opportunity for fraud, waste, and abuse.

FEMA Information Systems: (2005 and 2006)

2006 Accomplishments

- FEMA has completed a number of actions to implement recommendations contained in the Office of Inspector General's September 2005 report, Emergency Preparedness and Response Could Better Integrate Information Technology with Incident Response and Recovery (OIG-05-36).
- The Information Technology Services Division (ITSD) and FEMA program offices partnered with the Emergency Management Institute (EMI) to improve National Emergency Management Information System (NEMIS) training and guidance by developing a training plan and conducting field training and train-the-trainer activities.
- FEMA offers online NEMIS training and provides up-to-date system user guidance.
- FEMA created the Project Management Office to facilitate requirements gathering and communication.
- ITSD developed the Emergency Management Mission Integrated Environment (EMMIE) based on requirements collected by an interdisciplinary team and with all grant holders invited to participate.
- The Office of Inspector General just completed a review and assessment of FEMA's progress in implementing their recommendations, which is documented in their Draft Letter Report: *FEMA's Progress in Addressing Information Technology Management Weaknesses*. The letter noted that FEMA had made progress in many areas, particularly short-term modifications to prepare for the 2006 hurricane season. However, much work remains to address long-term IT and system development efforts. The Inspector General's letter stated that FEMA's resource challenges, including personnel needs, time limitations, and funding constraints, have a significant impact on implementing the Inspector General's recommendations. FEMA generally concurs with the assessment.
- The Chief Information Officer has reprioritized its resources to refine and refocus its efforts to address audit findings.

Continued on next page

Remaining Plans

- The Chief Information Officer will continue providing the Office of Inspector General with reports on the status of milestones on the unfinished Plans of Action and Milestones (POA&M) every 90 days.
- The Chief Information Officer holds bi-weekly meetings to ensure that progress is made on implementing the recommendations. The senior leadership of FEMA is committed to addressing the deficiencies in all audit reports and is monitoring progress under the POA&M during performance reviews.
- The Chief Information Officer is attending an off-site the end of October, after which plans will be reviewed, developed, or revised, as appropriate, to accomplish Agency goals.
- The Enterprise Architecture (EA) Office is staffing up to complete the remaining As-Is Enterprise Architecture in order to support analysis toward development of the Target EA. Portions of the Target EA are already underway. The EA Program Management Plan, containing a roadmap for full compliance with OMB EA Assessment Framework, is currently being updated. Additionally, regular meetings with the DHS EA Staff are conducted to ensure alignment with the DHS.

Flood Map Modernization Program: (2005 & 2006)

2006 Accomplishments

- FEMA performed a review of Flood Map Modernization, including input from Congress, GAO, Inspector General, and key mapping stakeholders. As a result, FEMA is implementing a Mid Course Adjustment designed to provide more accurate flood data while also producing digital flood maps for a significant portion of the Nation. FEMA reported on the Mid-Course Adjustment in the "Flood Map Modernization 2006 Report to Congress" dated February 10, 2006.
- Fully operational online capability for the Mapping Information Platform (MIP) was completed February 2006 for engineering/mapping tools, project management, data storage, and other functions.
- Work was completed with the USACE to successfully roll out a policy for provisionally accrediting levees that provides communities with additional time to gather data needed to assess the protective capabilities of levees while still allowing critical new flood hazard data to be released to communities to guide new development.
- FEMA collaborated with mapping stakeholders to update its plan for Flood Map Modernization to begin to reflect the Mid-Course Adjustment. The updated plan will be released in October 2006, providing a 60-day comment period to allow stakeholders to provide feedback.
- A new, web-based application within the Mapping Information Platform (MIP) was released on June 12, 2006 that enables licensed land surveyors and professional engineers to obtain an official map determination from FEMA in minutes. Traditional processes average several weeks.

Remaining Plans

- Digital Geographic Information Systems (GIS) flood data will be available for 50% of the nation's population in the first quarter of FY07.
- By the end of FY07, digital GIS flood data will be available for 60% of the nation's population, and 35% of the population will have effective, modernized maps.
- By the end of FY 2008, digital GIS flood data will be available for 70 % of the nation's population, and 50% of the population will have effective, modernized maps.
- Continue to increase stakeholders' awareness of and usage of risk data, providing mentoring and assistance to increase partner capabilities to mitigate risk, and improve customer service.
- Continue to assist and encourage states and local communities to partner with the Flood Map Modernization Program.

National Flood Insurance: (2006)

2006 Accomplishments

- The National Flood Insurance Program (NFIP) has had 26 consecutive months of uninterrupted net policy growth.
- For the first time ever, additional policy sales have resulted in more then 5 million flood insurance policies in force across this country under the NFIP.
- For the first time, over $1 Trillion of insurance is in force under the NFIP.
- The NFIP paid more than 160,000 NFIP claims from Hurricanes Katrina & Rita for almost $16 Billion, many times more than the highest previous amounts, in the more than 35 year history of the NFIP.
- Introduced new procedures that allowed for an expedited claims process to decrease the time needed to close claims for policyholders which allowed them to get paid for their losses more quickly.
- Developed and mailed comprehensive informational materials explaining what is, and is not, covered under the NFIP, as well as how claims are adjusted, to all existing and new (over 5 million) policyholders as required by the National Flood Insurance Reform Act of 2004.
- Developed the first ever formal NFIP claims appeal process for policyholders who may wish to challenge claims adjustments on their individual NFIP claims.

Remaining Plans

- Continue implementing and tracking program performance and effectiveness to ensure that sufficient cash reserves will be available to pay all losses and related expenses for the average historic loss year.

Contract Management: (2005 and 2006)

2006 Accomplishments

- Established internal control procedures for the contract administration and management of FEMA's Individual Assistance Program.
- For Individual Assistance Program, implemented training for proper contract administration procedures for FEMA's Program Offices and Contracting Officer Technical Representatives.
- Conducted internal acquisition review & procurement assessments of procurements of greater than $1 million prior to contract awards.
- Increased staffing level and warrant authorities of contract specialists

Remaining Plans

- Continue emphasis on establishing and disseminating policies and procedures for sound and proper acquisition functions. Established procedures will ensure consistency and adherence to prescribed polices and procedures.
- Continue training of contract administration procedures for individual assistance program.
- Continue to fill staffing level gaps and provide training opportunities to improve competency and contract specialists' certification levels.

Grants Management: (2005 and 2006)

2006 Accomplishments

- The FEMA Chief Procurement Officer (CPO) has developed a special monitoring plan to focus on the Katrina grants issues. This effort involves working with the FEMA regional offices to ensure that their monitoring of the Gulf Coast States is compliant with federal grants requirements. Appropriate analysis and follow-up are occurring. FEMA's Grant Office is the "premier" office and model for DHS.
- The CPO Grants Branch has an on-going quality assurance effort that reviews each quarter the regional office monitoring of state grant reporting.
- The CPO has developed a pilot effort to help states improve their sub-recipient monitoring and has field tested that pilot in two states.
- Grants management training has been held in both regional offices and long term field offices.
- A detailed review of the procurement practices of five sub-grantees was conducted.

Continued on next page

Remaining Plans

- Work with the Regional offices to increase their focus on grantee financial and progress reporting.
- Based on the positive results of the sub-grantees procurement reviews conducted for the Mitigation program, develop a grantee/sub-grantee procurement technical assistance process for the Public Assistance program.
- Work with the long term recovery offices to provide training and technical assistance and support their efforts to hire grants management specialists.
- Complete development of EMMIE (FEMA's Electronic Grants Disaster Systems) in FY07.

Managing Assistance and Housing for Evacuees: (2006)

2006 Accomplishments

- FEMA is expanding both on-line and telephone 800 number capacities to register up to 200,000 applicants daily and is pilot testing mobile registration intake centers.
- Real-time identification verification via contract with ChoicePoint is now in place on both FEMA's 800# and on-line registration systems. ChoicePoint is a contractor that provides identification verification services.
- A contract was placed that allows FEMA to issue authorization codes for hotel accommodations at the time of registration.
- FEMA has put in place a Memorandum of Agreement (MOA) with the Katrina Fraud Task Force headed by the U.S. Department of Justice's Criminal Division and the Assistant United States Attorney and consisting of numerous agencies' Offices of Inspector General to allow limited access to FEMA's Privacy Act Disaster Recovery Assistance Files for the purposes of identifying and investigating fraud cases.
- Recovery Strategy RS-2006-1, Mass Sheltering and Housing Assistance was published July 24, 2006. This strategy clarifies how FEMA will manage sheltering needs for catastrophic disasters, as well as coordination on out-of-state sheltering assistance.
- FEMA has developed the website Housing Portal (https://rims.fema.gov/hportal/home.htm). The Housing Portal consolidates rental resources for evacuees identified by federal agencies, private organizations, and individuals.
- FEMA has entered into a Matching Agreement with the U.S. Department of Housing and Urban Development (HUD) for a computer matching program that identifies FEMA applicants who are receiving excess or duplicate housing assistance from both FEMA and HUD.
- The National Shelter System (NSS), a web-based data system to allow users to identify, track, analyze, and report shelter data in a consistent and reliable manner, is operational.

Remaining Plans

- FEMA is working with the Office of Chief Counsel and other appropriate parties to engage other Federal partners, such as the Internal Revenue Service (IRS) and the Social Security Administration (SSA), for data-sharing that will not only prevent fraud but ensure proper assistance to registrants. FEMA continues to explore information sharing capabilities with the Department of Health and Human Services, the SSA, and the IRS.
- Outreach and user training for FEMA, the American Red Cross, State, and local governmental agencies is being undertaken to affect implementation of the NSS.
- NSS maintenance, improvements and usage will be ongoing and tested using real-time events.
- FEMA is developing planning guidance and will provide contract assistance to hosting States and local governments to plan for large scale mass sheltering and housing assistance.
- FEMA has convened a Disaster Housing Task Force to develop the necessary policies, procedures, and other documentation to support a fully functional and operational housing element under the National Response Plan's Emergency Support Function #6, Mass Care, Housing, and Human Services.
- FEMA is undertaking the Joint Housing Solutions Group and the Alternative Housing Pilot Program in the Gulf Coast States to identify test, and evaluate alternative housing options and strategies.

Continued on next page

- Mass Care and Housing standard operating procedures (SOPs) are being completed and updated at the national and regional levels. We anticipate conducting five regional workshops (with participation from two regional offices each) to update the regional SOPs.
- FEMA will be implementing provisions of the Post-Katrina Emergency Management Reform Act of 2006, which includes changes to the Housing program, an Individual Assistance Pilot Program, a National Disaster Housing Strategy, as well as other operational and program changes and strategy development requirements.

FY 2006 Challenge 2: Acquisition and Contract Management

FY 2005 Challenge 3: Contract Management

The report stressed the importance of monitoring adherence to ethical standards of conduct. It noted the shortage of trained program managers and a lack of a Department-wide policy. The Investment Review Board model needs improvements. The procurement function needs its undermanned staffing rectified and faces a challenge in managing several new large and complex programs. A comprehensive independent oversight program is needed.

Standards of Conduct / Ethical Conduct: (2005 and 2006)

2006 Accomplishments

- Participation of senior program and procurement officials in management and ethics training.

Remaining Plans

- Completion of senior program and procurement officials' management and ethics training. (Target date Q1 FY07).

Program Management Training / Comprehensive Acquisition Guidance: (2005 and 2006)

2006 Accomplishments

- Dissemination of the Acquisition Professional Management Directive to identify and certify appropriately trained and experienced program managers, contracting officer technical representatives, and authorized buying agents. DHS has certified 348 Program Managers since 2004 and continues to focus on qualifications and placement (completed Q3 FY 04, ongoing).

Remaining Plans

- Support leadership and innovation in federal acquisition and apply best practices to DHS procurements: Department participation in the knowledge management portal, which provides federal agency guidance on procurement policy and procedures, will in turn provide DHS with information related to emergency incident policies and procedures, the availability of Interagency Agreements, and training opportunities. Finally, the recently published FEMA Emergency Acquisition Field Guide will clarify Department and service provider roles and responsibilities (target completion date Q1 FY 07).

Investment Review Board Process: (2005 and 2006)
2006 Accomplishments • Established a Program Management Council to improve program management practices among DHS Components. The Council provides a forum for discussion and sharing of best practices, improves the quality and consistency of Program Management across the department, and supports expansion of the acquisition career field to other areas of expertise (e.g. Information Technology, Logistics, Finance, Testing, etc). • Improved the DHS management directive for investment review processes by providing greater clarity on DHS policies and procedures. This Management Directive (MD) establishes the Investment Review Process (IRP) to provide Departmental oversight of major investments throughout their lifecycles and to identify cross-programmatic efforts. Developing and maintaining the capability needed to achieve Department of Homeland Security (DHS) missions requires a robust investment program. • Prepared a DHS Investment Management Handbook guide to the Investment Review Process (IRP) and supplements Management Directive (MD) 1400, Investment Review Process. It contains guidelines, time frames, and charters to assist projects in understanding and implementing the directive. The focus is on explaining how the process works, defining the roles involved further than discussed in the MD 1400, and providing the templates that facilitate the process so that the IRP can become an integral part of the management of the investment. • DHS components are now required to report in status of major investments quarterly. Information is submitted to ensure investments are staying within established baselines for cost, schedule and performance. Information is also collected to achieving program manager certification and establishing a compliant earned value management system.
Remaining Plans • Strengthen contract review and administration to ensure that products and services meet contract requirements: The Department will identify and introduce acquisition best practices into the investment review process (target completion date Q1 FY 08).

Procurement Staffing: (2005 and 2006)
2006 Accomplishments • Correcting the misalignment between Department contract spending and procurement staffing levels (target completion date Q4 FY 09).
Remaining Plans • Build the DHS acquisition workforce to enhance the Department's acquisition program: DHS initiatives to resolve personnel shortages will include a centralized recruiting system for contract personnel within DHS components, an Acquisition Fellows Program that includes the recruitment of college graduates, and out-year budget requests for increased staffing levels (target completion date Q4 FY 08).

Procurement Management & Reviews / Providing Accurate and Timely Procurement Reporting: (2005 and 2006)
2006 Accomplishments • Implementation of Strategic Sourcing Commodity Councils to review and leverage the Department's buying power (ongoing).
Remaining Plans • Establish acquisition systems with well-defined missions and qualified management teams: DHS will put integrated project teams and business processes in place to facilitate sound program management and effective contract administration. This will help ensure adherence to program cost schedule and performance parameters (target completion date Q4 FY 07).

Procurement Oversight: (2005 and 2006)
2006 Accomplishments • Increasing the number of appropriately certified program managers who provide oversight for key DHS investments (ongoing)
Remaining Plans • Centralizing and linking procurement processes to financial systems for improved contract administration and vendor payments (target completion date Q 4 FY 08)

FY 2006 Challenge 3: Grants Management
FY 2005 Challenge 4: Grants Management The report indicates that DHS needs to ensure homeland security assistance is targeted at the areas of highest risk/vulnerability. Internal coordination was lacking, did not fully address infrastructure protection priorities and thus low-scoring projects were funded. The grant evaluation process is another area of improvement opportunity, especially to ensure post-award administration tracks to DHS objectives. SLGCP is expected in FY05 to increase staffing in some areas.

Homeland Security Assistance and Grants Award Determination: (2005)
2006 Accomplishments • A risk-based grant allocation process was completed in the third quarter of 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. • The National Infrastructure Protection Plan (NIPP) was completed. Recognizing that the vast majority of the nation's critical infrastructure is owned and operated by private industry or state, local, and tribal governments, the NIPP formalizes critical infrastructure protection roles and responsibilities and strengthens existing critical infrastructure partnerships. The NIPP focuses on seventeen critical infrastructure and key resource (CI/KR) sectors as defined in Homeland Security Presidential Directive 7 encompassing but not limited to the following areas: agriculture and food; energy; public health and healthcare; banking and finance; drinking waters and shipping; transportation systems including mass transit, aviation, maritime, ground or surface, and rail and pipeline systems; chemical; commercial facilities; government facilities; emergency services; dams; nuclear reactors, materials and waste; the defense industrial base; and national monuments and icons. • The National Strategy for Homeland Security attaches special emphasis to preparing for catastrophic threats with "the greatest risk of mass casualties, massive property loss, and immense social disruption." To prepare for such threats, National Planning Scenarios were developed to illustrate the potential scope, magnitude, and complexity of a plausible range of major events, including terrorist attacks, major disasters, and other emergencies. The scenarios are not intended to be exhaustive or predictive; rather, they are meant to illustrate a broad range of potential terrorist attacks, major disasters, and other emergencies and their potential for creating damage. *Continued on next page*

Remaining Plans

- Completion of the National Preparedness Goal in FY 2007 with measurable readiness targets that appropriately balance the potential threat and magnitude of terrorist attacks, major disasters, and other emergencies with the resources required to prevent, respond to, and recover from them." Risk-based target levels of capability will meet that requirement. The intent is to establish capability baselines for operational missions and track resource allocation against them.
- A National Response Plan Review and Revision is targeted for completion in FY 2007. The Plan will integrate federal, state, and local lessons learned from the 2005 hurricane season in order to better prepare for catastrophic incidents nationwide. While most areas of the country are well prepared to handle standard disaster situations, DHS' assessment of nearly 2,800 emergency operation plans from across the country determined the need for all levels of government to improve emergency operations planning for catastrophic events such as a major terrorist attack or a category-five hurricane strike. The Department has established a National Preparedness Task Force that will oversee central DHS efforts to strengthen and systematize catastrophic planning. This office will maintain expertise in the prioritization of actions and resource planning efforts among all levels of government that will be best translated into nationwide enhancements for catastrophic planning.
- Require States and urban areas to revise their Homeland Security Preparedness Strategies and submit fully updated strategies pursuant to the National Preparedness Goal in order to receive further Federal preparedness assistance (ongoing). In accordance with HSPD-8, updated strategies were originally aligned to the National Preparedness goal in early FY06.
- Broaden its risk and assessment focus to address additional risk-based priorities in FY 2007.

Grant Post-Award Administration / Monitoring Grantee Financial Accountability/ Tracking Progress to DHS Grant Objectives / Monitoring Outcomes/ Staffing - Site Visits & Project Oversight : (2005 and 2006)

2006 Accomplishments

- The Office of Grants and Training (G&T), a component of DHS's Preparedness Directorate, is responsible for preparing the nation against terrorism by assisting states, local and tribal jurisdictions, and regional authorities as they prevent, deter, and respond to terrorist acts. The Office published its first *Financial Management Guide*. The guide, which serves as a resource for all G&T grantees, streamlined previous requirements, eliminated unnecessary prohibitions, and provided clarification of terms in relationship to DHS/G&T activities.
- Conducted 10 financial management workshops and other training opportunities to establish a baseline skill set for G&T grantees and to assist grant recipients to strengthen accountability in the management and administration of G&T grant resources. Specifically these workshops focused on G&T's overall award process, including Grants.gov requirements; a review of federal reporting requirements, terms and conditions; major procurement and contracting activities; and monitoring responsibilities.
- Conducted 20 on-site financial monitoring visits in tandem with G&T program staff. This level of monitoring was unprecedented and reflects the significance of G&T taking ownership of its post-award activities. It is important to note that, through its monitoring efforts, OGO is not finding waste, fraud and abuse by grantees, but rather that state financial managers are challenged to correctly record transactions funded with federal homeland security grant resources.

Remaining Plans

- A priority in FY 2007 is to refine internal grant management activities in the areas of training, technical assistance, and post-award monitoring. Specifically, G&T is leveraging its expertise and will co-sponsor 11 regional workshops called: G&T Grants Management Solutions. These workshops will provide grantees with more advance learning opportunities and is the direct result of grantee input and feedback.
- In FY 2007, G&T will be initiating an effort to streamline its programmatic and financial monitoring protocols and activities. The desired end result will be a unified G&T Monitoring Program that will appropriately address Inspector General concerns regarding DHS's ability to monitor the preparedness of state and local governments, grant expenditures, and grantee adherence to the financial and programmatic terms and conditions of homeland security grants.

FY 2006 Challenge 4: Financial Management
FY 2005 Challenge 5: Financial Management This section of the report focuses on the auditors' disclaimer of opinion on DHS' consolidated financial statements. It specifically calls out "significant financial funding problems" centering around ICE and USCG reporting deficiencies.

This challenge coincides with the High Risk Areas reported by the Government Accountability Office. Corrective action plans have been developed to overcome the weaknesses identified in the Inspector General's report. A summary of corrective plans for material weaknesses in internal controls are found in the Management's Discussion and Analysis (MD&A) portion of the Analysis of Internal Controls, Systems, and Legal Compliance section.

FY 2006 Challenge 5: Information Technology Management
FY 2005 Challenge 7: Integration of Information Systems The report points out the major challenge of creating "a single infrastructure for effective communications and information exchange at various classification levels." The Office of the Inspector General expects that the DHS Transformation Program will encompass all support services. The Office of the Chief Information Officer, however, does not yet have authority, mission scope and staffing to strategically manage DHS component assets and programs.
FY 2005 Challenge 8: Security of Information Technology Infrastructure The report reiterates directives by the Federal Information Security Management Act (FISMA) to develop and implement a Department-wide information security (IS) program. Work needs to be completed at the Component level to adhere to new Department policies, procedures and practices. Examples are to complete certification and accreditation (C&A). The Components' Plans of Action all need to be completed and the enterprise management tool data updated. More effort is needed to provide adequate security for classified systems' information security.

Information Technology Infrastructure Transformation Program: (2005 and 2006)
2006 Accomplishments • Under a data consolidation effort located at Stennis Space Center in Mississippi, Data Center Services completed construction Phase I (24k sq ft) on time. • Data Center Services completed the first transition of a component system to Stennis.
Remaining Plans • Consolidate IT and technology infrastructure to unify business processes across lines of business. Consolidations include reducing seventeen data centers to two, reducing seven area networks to one, and reducing multiple email platforms to a common platform.

Office of the Chief Information Officer (OCIO) Component Information Technology (IT) Program Management: (2005 and 2006)
2006 Accomplishments • DHS Strategic Plan goals have been carried forward through the Management Directorate Strategic Plan.
Remaining Plans • The Office of the Chief Information Officer will develop and promulgate the IT Strategic Plan (target completion date Q2 FY07).

Office of the Chief Information Officer Insufficient Staffing: (2005)
2006 Accomplishments • Hired 21 new employees in FY2006. The Office of the Chief Information Officer is now staffed at 70%.
Remaining Plans • Increase certified project managers on all key and major investments (target completion date Q1 FY07). DHS Program Managers must be certified at a level commensurate with the responsibilities of the acquisition being managed or eligible for certification within 18 months of designation. • Ensure that all contracts have a certified Contracting Officer's Technical Representative (COTR) (target completion date Q4 FY07).

Federal Information Security Management Act Compliance / Department-wide program: (2005 and 2006)
2006 Accomplishments • Of the 700 systems identified 94% have been certified per the Federal Information Security Management ACT. Grades improved from an F to C-.
Remaining Plans • Continue to certify remaining systems. • Ensure that policies are updated and enforced

FY 2006 Challenge 6: Infrastructure Protection
FY 2005 Challenge 9: Infrastructure Threat Assessment • The report indicates a precursor to assessments is the fielding of the National Assets Database and codification of the processes that populate it.

National Assets Database (NADB) Processes and Policies: (2005)
2006 Accomplishments • NADB-Secret production system was accredited and granted an Authority to Operate by DHS and the Department of Energy. • Implemented the Gross Consequence of Attack Tool Version I and began analysis on all viable NADB assets. • Updated NADB-Secret production system with improved functionality and capabilities to include ICAV integration. • Conducted 12 Expert Panels to refine data collection framework, develop criteria delineating assets of national importance, and define data elements of interest for specific asset categories. • Initiated a data call to State Homeland Security Advisors to validate list of nationally significant assets (Tier Two) for focus of FY07 resource allocation and infrastructure protection efforts.
Remaining Plans • In FY07, the NADB will be restructured into the Infrastructure Information Collection Program (IICP), which will encompass capabilities and functionalities of four previously independent projects: Automated Critical Asset Management System (ACAMS), Risk Analysis and Management for Critical Asset Protection (RAMCAP), Vulnerability Identification Self Assessment Tool (VISAT), and the NADB. The IICP will develop, implement, and standardize a model system for the automated collection of standardized infrastructure information from private sector owners/operators, local law enforcement and first responder communities, federal partners and commercial vendors to provide a coordinated strategy and methodology to collect the quantitative, asset-specific variables required to draw reliable, risk-based conclusions. • Codify the data standards and formats for promulgation across data collection efforts to ensure consistency in information as well as leveraging existing capabilities to improve efficiencies in collection.

NADB Data Population: (2005 and 2006)
2006 Accomplishments
• Data Calls conducted in coordination with Sector Specific Agencies (SSA) and State and Territorial Homeland Security Advisors (HSA) to identify infrastructures of national significance/criticality. • Developed Rapid Ingest Model concept for the automated integration of disparate data from varying sources and formats. Provides for the rapid consolidation of information into single composite records.
Remaining Plans
• Under the framework of the National Infrastructure Protection Plan (NIPP), continue efforts with the Sector Specific Agencies and State and Territorial Homeland Security Advisors to identify existing sources of information and means for additional collection. Data calls will be made with continued verification of collected data.

FY 2006 Challenge 7: Border Security
FY 2005 Challenge 10: Border Security The report lists several challenges, beginning with development of an automated entry-exit system (United States Visitor and Immigrant Status Indicator Technology - US-VISIT) and encompassing illegal alien issues, law enforcement-supporting technologies, intelligence support, overseas operations and the immigration benefit application backlog. The inability of Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) to better coordinate is cited.

United States Visitor and Immigrant Status Indicator Technology - US-VISIT System Development: (2005 and 2006)
2006 Accomplishments
• The US-VISIT system continued biometric identification services and support of the Department of State's Consular Offices, Customs and Border Protection officers, Immigration and Customs Enforcement agents, and Citizenship and Immigration Services officers. It extended the identity verification capabilities of the US-VISIT Integrated Automated Fingerprint Identification (IDENT) system to cover the full complement of northern and southern land border ports of entry; • prepared for the operational deployment of the electronic passport or e-Passport readers based on standards set by the International Civil Aviation Organization in response to the legislative mandate; • continued to refine and improve the services from the Automated Biometric Identification system to stakeholder agencies; completed the deployment of the transition of fingerprint standard (10-print) and the interoperability of two biometric systems to support enforcement actions within the interior of the United States and its borders; provided information through analytical services that contributes directly to border security and immigration integrity; and engaged in information and technical assistance, both domestically and internationally to support shared and interoperable information sharing furthering the extension of the virtual border of the United States. • At Land Border Ports extended coverage to the full complement of ports and conducted pilots of Radio Frequency Identification Device (RFID) Capabilities. • Completed the deployment of the IDENT/IAFIS 10-print rolled capability to support enforcement actions to ICE and CBP Field Offices;
Remaining Plans
• US-VISIT will continue to deploy biometrics functionality that will expand its contributions to safeguarding the nation and ensuring the integrity of the immigration and border management systems. The program will focus on the mission activities in deployment of passport readers which fulfills the congressional requirement for installing scanners at ports of entry to read biometric e-Passports; evaluation of technologies for biometrically enabled radio frequency identification tokens to enable the remote validation of identity management on exit through the land borders. *Continued on next page*

- Development of a comprehensive exit strategy for the air, sea and land environment
- Continue migration to a new 10-fingerprint standard for enrollment and the interoperability of two major biometric data repositories.
- Continue education of stakeholders, both internal and external, to ensure compliance with new requirements; and respond to requests from federal departments, agencies and foreign governments for assistance in the implementation of biometric capabilities.

Fielding Border Surveillance Technologies / SBInet Program Management: (2005 and 2006)

2006 Accomplishments

- Award of the Prime Integrator Contract to Boeing.
- Establishment and staffing of the SBInet Office and establishment of a new organizational structure to ensure proper contract and program oversight.
- SBInet replaces and expands upon two previous efforts to gain control of the borders: the Integrated Surveillance Intelligence System (ISIS) and the America's Shield Initiative (ASI).

Remaining Plans

- Deploy SBI.net, an integrated technology system in support of the Secure Border Initiative (SBI), and expand staff and tactical infrastructure to achieve operational control (target completion date Q4 FY08).
- Continue to increase staffing levels within the SBInet office with professional program management personnel.
- Present the defined requirements to the Joint Requirements Council and the Investment Review Board.

Providing Intelligence to Border Security Operations: (2005 and 2006)

2006 Accomplishments

- Physically modified the CBP Sensitive Compartmented Information Facility to increase the number of classified computer terminals and improve analyst access to intelligence reporting.
- Increased on-site intelligence support at the National Targeting Center (NTC) to provide 24x7 coverage.
- Worked with DHS/Intelligence & Analysis counterparts to articulate detailed intelligence requirements to the intelligence community resulting in a significant increase in the quantity and relevancy of classified intelligence reporting received at CBP.
- Partnered with the Department's Office of Intelligence and Analysis to imbed four "report writers". These writers review CBP operational reporting, identify information of national intelligence value, and prepare and disseminate Homeland Information Reports (HIR). CBP information now accounts for approximately 80% of the Department's HIR reports.
- Partnered with the Department's Office of Intelligence and Analysis to deploy a Homeland Intelligence Support Team (HIST) to El Paso for about a one-year period. This team will develop best practices to serve as a model for future HIST support to specific homeland security challenges; similar to the National Intelligence Support Team (NIST) concept developed by the National intelligence Community.

Remaining Plans

- Expand the CBP Sensitive Compartmented Information Facility to not only increase work space but also to create collaborative work areas for analysts and operators to work joint analytic projects.
- Pilot two field intelligence units beginning in January 2007. The goal of these pilots is to integrate and co-locate operational and intelligence specialists, fuse operational reporting with intelligence, and focus intelligence production on support to the tactical officer and field manager. Simultaneous to the field pilots, a dedicated team of analysts will provide tailored national level intelligence to the pilot units. The pilots will also develop best practices for improving the field-level intelligence requirements process.

Immigration Benefit Application Backlog: (2005)
2006 Accomplishments
• The U. S. Citizenship and Immigrations Service (USCIS) nearly eliminated the entire immigration benefit application backlog.
Remaining Plans
• To prevent future backlogs, USCIS is embarking on an enterprise-wide "Transformation Program" that will transition the agency from a fragmented, paper-based operational environment to a centralized and consolidated environment, utilizing electronic adjudication. The Program is a large-scale, complex undertaking that will form the foundation of USCIS-wide business processes and Information Technology enabled re-engineering.

Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) Interoperability (2005 and 2006)
2006 Accomplishments
• The Second Stage Review of DHS (2SR) provided the Secretary with direct ability to ensure his top operational priorities are being addressed, both by CBP and ICE, as well as the other operational components. • Establishment of CBP and ICE Coordination Council to improve relations and coordination by bringing together the two agency heads and their key operational leaders for discussions of issues of common concern. • Creation of CBP and ICE field leaders working group. The charter for this group includes guidance on discussing issues of common concern, such as participation in the Joint Terrorism Task Force, improving information sharing in the field, updating policy on controlled deliveries, and the CBP Officer-Enforcement program.
Remaining Plans
• Reach consensus on the Addendum to the November 16, 2004, CBP and ICE Joint Memorandum of Understanding, which is currently under draft by CBP Border Patrol Sector Chief's and ICE Special Agents-In-Charge. The Addendum will strengthen the working relationship, and clarify roles and responsibilities at the field level. • Define and coordinate roles and responsibilities of CBP and ICE personnel in U.S. embassies and consulates.

FY 2006 Challenge 8: Transportation Security
FY 2005 Challenge 11: Transportation Security The report specifies a continuing need for detecting explosives on the human body. The United States Coast Guard (USCG) faces a known major challenge to perform its legacy missions, implement the Maritime Transportation Security Act of 2002 (MTSA), maintain its deep water fleet and to better develop its infrastructure.

Detection of Explosives on a Human Body / Screening Performance: (2005 and 2006)
2006 Accomplishments
• Implementing multiple layers of security, the Transportation Security Administration (TSA) continually provided its dedicated Transportation Security Officer (TSOs) workforce with the technology, training, and operational procedures they need to effectively carryout their responsibilities for screening passengers and baggage at our Nation's airports. To strengthen the ability to detect explosives at security checkpoints, TSA enhanced explosives detection training for TSOs in both the classroom and hands-on experience in identifying X-ray images of improvised explosive device components. Additionally, TSOs are being trained and certified as Bomb Detection Officers in the screening of passengers by observational techniques. New standard operating procedures encourage TSOs to work together more than ever before to find items that may pose a security threat. *Continued on next page*

Remaining Plans

- TSA will continue to expand efforts toward development and deployment of emerging screening technologies to improve the automation of threat detection baggage screening. TSA has conducted several pilot programs at airports nationwide, such as the explosive trace portal and the explosive detection document scanner to facilitate enhanced TSO performance.

USCG Deepwater Program: (2005 and 2006)

2006 Accomplishments

- The Coast Guard has taken disciplined steps to ensure that its Deepwater acquisitions remain within cost, schedule, and performance baselines. Currently, Deepwater will complete the recapitalization of the Coast Guard's cutter fleet with a system-of-systems in 25 years at an acquisition cost of $24 billion. This baseline discipline has been achieved by stabilizing requirements, increased cost control, and persistent Coast Guard oversight of subcontractors.
- In 2006, a new award term criteria was developed that placed greater focus on cost control through more appropriate contract type selections, the use of performance incentives within each order, and the use of award fees to support the award term criteria.
- Finally, the Coast Guard will ensure Deepwater crews are properly trained and supported on these new assets to assure peak operational performance.
- The Coast Guard has implemented increased oversight of the requirements process to ensure that contractor activities meet program goals and objectives under this unique performance-based contract structure. This has been done by the establishment of domain management teams that serve as oversight and conflict resolution entities while they enhance collaboration on issues that cut across several areas. These teams have allowed the Coast Guard to improve increased communications with the system integrator and first-tier subcontractors so that requirements are more easily discernable.
- The Coast Guard has now updated its Deepwater Measures of Success (MOS) to now emphasize improvement of output performance (cost, schedule, and deliverable performance to plan) while retaining fundamental success measures (charters, training, participation) that are required to sustain consistent and effective performance.
- The Coast Guard has codified and streamlined the review of proposed Deepwater design changes, via an updated Proposal Development Process that incorporates initial sponsor review and approval of new or changed requirements.
- The Deepwater program's Configuration Management Plan (CMP) as well as the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) management plan were updated in 2006 to support the clear communication of requirements, as well as to capture and describe how such processes fit within overall Deepwater program responsibilities.
- The Coast Guard has outlined a best practice security build approach for layered applications starting at the operating systems level and mitigating vulnerabilities at the various layers. This layered approach implemented during the changes leading to the WPB-123 project to achieve Authority to Operate in 2006.
- The Coast Guard has used outside resources to better mitigate and resolve previous vulnerabilities through use of bodies such as the Space and Naval Warfare Systems Command (SPAWAR) that has been actively working on identifying and mitigating vulnerabilities in the Deepwater program. The use of such assistance has led to the C4ISR Integrated Support Plan being modified from a semi-annual asset software update to a quarterly update to meet vulnerability mitigation time lines.

Remaining Plans

- The Coast Guard will continue to pursue a schedule that puts its newly designed Fast Response Cutter (FRC) on a schedule to be "ready for operations" in 2010, but will also concurrently explore other options such as "off-the-shelf designs" that may allow the FRC to meet a "ready for operations" deployment in FY 2009.

Continued on next page

- The Coast Guard has ended the conversion of eight patrol boats into new 123-foot patrol boats that did not meet post September 11, 2001 service needs. The Coast Guard intends on pursuing a Service Life Extension Program for its 110-foot cutters as a bridging strategy until the FRCs are delivered.
- The Coast Guard has adjusted its Vertical Takeoff-and-Landing Unmanned Aerial Vehicle (VUAV) program with plans to acquire one air vehicle, one ship control station, and one ground control station in FY 2007. The Coast Guard will also conduct additional tests in FY 2007 between the air vehicle and its two control stations.
- The Coast Guard's HH-65 Conversion to Multi-Mission Cutter Helicopters (MCH) has been affected by higher than anticipated cycle times which have dictated a shift in the conversion schedule that will see the completion date for all 84 operational aircraft to be re-engined in FY 2007.
- The Coast Guard is currently reviewing the curriculum for the nine courses being developed for C4ISR users and is engaged and assisting in plans to have appropriate resources for initial and follow-on training. The Coast Guard believes that most of the Deepwater training data used by the DHS Office of Inspector General appears to have been captured from WPB-123 crews, and was based on the initial training conducted. Many of the issues and comments included in this report were previously captured as part of four Coast Guard-led after training "hot wash" activities and have already been incorporated into subsequent training evolutions.

USCG Infrastructure Development: (2005)

2006 Accomplishments

- The Coast Guard believes that it has made steady progress over the past year in implementing Deepwater's revised production plans and that these plans, based on a comprehensive performance-gap analysis, are well-aligned with the Department of Homeland Security's strategic goals/priorities, the National Strategy for Homeland Security, and the new National Strategy for Maritime Security. The revised plan ensures that Deepwater cutters and aircraft will be equipped with the right systems and capabilities to operate successfully in all mission areas in the face of a more challenging post-9/11 threat environment.
- The Coast Guard achieved a significant milestone with the completion of step-two C4ISR upgrades aboard all 210-foot, 270-foot and 378-foot cutters, with the USCGC MORGENTHAU (WHEC-722) being the last legacy cutter of thirty-nine to be upgraded with Automatic Identification System and INMARSAT-B installations as well as upgraded Law Enforcement radio capabilities.
- The first National Security Cutter, the USCGC BERTHOLF, was launched on Sept. 29, 2006, while the keel for the second NSC, the USCGC WAESHE, was laid on Sept. 11, 2006.
- The delivery of the eighth Short Range Prosecutor (SRP) in January 2006 coincided with the delivery of the eighth and final 123-WPB in 2006.
- Lockheed Martin and aircraft maker EADS CASA rolled out the first production airframe of the HC-235A medium range surveillance maritime patrol aircraft.
- The Coast Guard's HC-130J Missionization project successfully passed its Preliminary Design Review held in Moorestown, NJ.
- The Coast Guard conducted its first successful flight of a full-scale risk reduction demonstrator of the Vertical Take-off and Landing Unmanned Aircraft Vehicle (VUAV).
- The Coast Guard designated 43 Boat Force Stations as Heavy Weather Stations and established heavy weather staffing standards to better provide an all-weather response. Similarly, the Coast Guard instituted a Surf Station staffing standard to ensure that search and rescue coxswains are better prepared to encounter severe sea and surf states, as well as increased training quotas and established a service Boat Forces Doctrine Command which has instituted fleet-wide materiel inspections to improve small boat readiness.
- The Coast Guard deployed new motor lifeboat simulators as well as seven additional boat training platforms to more efficiently provide crucial rescue training conditions, and has instituted a common and standard navigation equipment suite to reduce lost time learning unique equipment.
- The Coast Guard has expanded small boat senior enlisted command ashore training to include engineering rates in order to improve real-time crisis management decisions by a safe and effective leadership team.

Continued on next page

- The Coast Guard deployed Rescue 21 national distress VHF marine radio systems in two additional major recreational boating areas - Mobile, Alabama, and St. Petersburg, Florida - to enhance radio and direction finding capability to receive and pinpoint the location of maritime distress calls.
- The Coast Guard completed development of a new search and rescue planning tool for Rescue Coordination Centers and Sector Command Centers – known as the Search and Rescue Optimized Planning System (SAROPS). This program has greatly improved existing maritime search planning tools by drawing upon a number of external factors that can be used to determine optimum search areas.
- The Coast Guard has developed and deployed a Common Operational Picture capability on its large afloat platforms and shore-side Command Centers. This has improved service performance by allowing operational commanders make better strategic and tactical decisions that ensure more effective resource utilization.

Remaining Plans

- Changes to the Deepwater Implementation Plan in the President's fiscal year 2007 budget request will align the acquisition and projected delivery of Deepwater end-state assets so that assets, information systems and shore facilities are sequenced to provide operational capability as soon as practical. Useful segments are re-phased to complement this approach. The executable line items requested in the President's fiscal year 2007 budget request have been synchronized to provide increased operational performance compared to 2005 projections.
- Actual year-end asset performance projections in the out-years will be thoroughly evaluated during Operational Test and Evaluation to validate the projected number and capabilities of Deepwater assets to meet the Mission Need Statement (MNS) as revised in 2005
- The VUAV project plan has been adjusted, and one air vehicle, one ship control station, and one ground control station can be procured with the funds appropriated in fiscal year 2006. With the additional funding, additional testing will be conducted during fiscal year 2007 primarily between the air vehicle and the two control stations.
- Changes to HH-60 budget allocation correspond with the higher operational priority for the HH-65/MCH conversion. The existing HH-60funding will support avionics replacement, continue the required funding for the HH-60 Service Life Extension Project (SLEP), continue funding for the HH-60 radar/Forward Looking Infra Red (FLIR) replacement, and fund HH-60 engine sustainment. Future-year funding will be used to start the HH-60 Post-9/11 Capability Upgrades, as well as complete the HH-60 avionics replacement, HH-60 SLEP, HH-60 radar/FLIR replacement, and HH-60 engine sustainment.
- The Coast Guard will continue to deploy Rescue 21 national distress VHF marine radio systems to the Pacific Northwest and Mid-Atlantic regions in 2007.
- The Coast Guard will deploy the SAROPS system nation-wide in 2007.
- The Coast Guard will install Automated Identification Systems transponders and Blue Force (friendly-force) Tracking equipment on all of its Small Boats to increase encrypted situational awareness that will enhance mission performance.
- Internet data connectivity will be installed on several Coast Guard Patrol Boats in 2007, providing global data connectivity that will contribute to enhanced mission execution by providing underway access to Enterprise Applications such as MISLE, situational awareness tools such as the Common Operations Picture (COP), and newly developed mission specific operational tools such as biometric data exchange.

TSA Rail and Mass Transit Security: (2006)

2006 Accomplishments

- TSA made significant progress employing a dynamic strategy to ensure the security of mass transit and passenger rail focused on regional engagement, expansion of explosives detection capabilities, and maximizing the impact of available security resources through random, visible security activities. Working with its government partners, industry owners, and operators to improve security for transportation modes other than aviation, TSA has increased its emphasis on building information sharing networks; appointed general managers for each critical transportation area; deployed Federal Security Compliance Inspectors for rail and mass transit facilities; deployed Canine Explosive Detection Teams for mass transit; and conducted security exercises and training.
- TSA led efforts to organize the Transit, Commuter, and Long distance Rail Government Coordinating Council to develop consistent and effective security strategies and programs.

Remaining Plans

- TSA will continue to increase its vigilance through more robust information sharing, threat detection, and enhanced coordination among Federal, State, and local government entities and private sector partners to ensure the security of the transportation systems.

FY 2006 Challenge 9: Trade Operations and Security

FY 2005 Challenge 12: Trade Operations and Security

The report refers to a previous one on the Automated Targeting System (ATS), which evaluates the trade supply chain and its vulnerabilities. That report indicated improvements are needed to the data to which ATS targeting rules apply, that targeting rules use examination results and to improve physical control over containers. The report notes that the ATS review is legislatively mandated.

Customs-Trade Partnership Against Terrorism (C-TPAT)

2006 Accomplishments

- Conducted 1,887 validations, which resulted in 3,387 total numbers of validations completed, or 55% of the certified membership--an increase over the 27% validation level in FY 2005.
- Added 65 permanent Supply Chain Security Specialists--up from the 60 on board in FY 2005.
- Established minimum-security criteria for sea, highway and rail carriers, and foreign manufacturers.
- Implemented the web communications portal for all members and applicants.

Remaining Plans

- Complete 2,750 validations in FY 2007.
- Hire an additional 31 permanent Supply Chain Security Specialists.
- Establish minimum-security criteria for air carriers, brokers, terminal operators, freight forwarders and consolidators.

ATS Targeting Rule Revisions / Automated Targeting System: (2005 and 2006)

2006 Accomplishments

- Incorporated new weight sets for targeting initiatives related to risks in the areas of pharmaceuticals, Intellectual Property Rights (IPR), and agro-terrorism.
- Coordinated with the U.S. Postal Service (USPS) to develop a pilot for an automated targeting solution for outbound mail.
- Incorporated analysis tools in support of targeting strategic and tactical post seizure analysis that identified suspect vehicles and registered owners that were or may be engaged in mala fide activity.
- Incorporated enhancements to allow Border Patrol Agents the ability to easily perform research queries in a single federated query, compiling data from multiple TECS modules as well as the ENFORCE system.

Remaining Plans

- Continue to work with USPS in the mail environment on the inter-operability of the different systems and the requirements for targeting rules, which have been developed, but are awaiting a resumption of the operational pilot--currently scheduled for January 2007.
- Continue to develop the Simulation and Testing Environment to provide a robust rules and system evaluation tool for ATS.

Automated Commercial Environment (ACE)

2006 Accomplishments

- ACE electronic truck manifest capabilities are operating at 49 land border ports, including every land border port on the Southern Border.
- More than 150 users from 16 participating government agencies are using ACE to access trade data, including more than 30 reports that draw from entry and entry summary data.
- Periodic monthly statement receipts grew to $747.8 million, representing 30 percent of total adjusted collections. Overall, there are more than 3,500 ACE Secure Data Portal accounts, and 3,915 corporate entities are approved to pay duties and fees monthly – bringing calendar year 2006 growth in entities approved for Periodic Monthly Statement to more than 210 percent.

Remaining Plans

- Complete deployment of ACE truck processing capabilities by the end of May 2007.
- Implement a mandatory e-manifest policy on a port-by-port basis.
- Develop and prepare new ACE capabilities that will further strengthen screening and targeting efforts and streamline operations for CBP officers and the trade community.

Container Security Initiative (2005)

2006 Accomplishments

- Reached a milestone of 50 Operational CSI ports, covering 82% of U.S. bound maritime containers.
- Transitioned 12 CSI ports to permanent staffing, bringing the total number of posts with permanent personnel to 28.
- Increased the level of examinations conducted at CSI locations by 77%.
- Finalized the CSI Strategic Plan and updated the Human Capital Plan.

Remaining Plans

- Open 8 additional CSI ports, bringing the total number of CSI operational ports to 58 covering approximately 85% of containerized cargo destined to the United States.
- Establish remote targeting pilot project with real-time remote imaging and live video of the inspectional process.

U.S. Coast Guard (USCG) Implementation of Maritime Transportation Security Act of 2002: (2005)

2006 Accomplishments

The Coast Guard has:

- Partnered with TSA in their effort to establish a Transportation Worker Identification Credential (TWIC) to vet all workers associated with commercial ports. While TSA will be responsible for issuing cards to approximately 1,000,000 port and domestic vessel employees, the Coast Guard will handle enforcement of the program by requiring all persons who are deemed to need unescorted access to the secure areas of regulated vessels and facilities possess a valid TWIC.
- Has negotiated international training requirements at the International Maritime Organization (IMO) for ship, facility, and company security officers for inclusion into international IMO Conventions, and is also currently negotiating similar training requirements for other vessel personnel at the IMO.

Continued on next page

- Worked with the U.S. Maritime Administration to develop security training standards for governmental ship and facility personnel. In addition, voluntary agreements have been instituted for these officers to undergo Coast Guard approved training programs.
- Continues to make progress in approving over 3,100 Facility and 11,000 Vessel Security Plans, over 4,700 of which have been further refined since their initial review.
- To ensure American commercial ships comply with required MTSA security requirements, the Coast Guard has conducted over 9,000 verification examinations on over 85% of the approximately 10,000 U.S. registered commercial ships.
- Led a National Maritime Recovery Symposium to further explore ways to ensure rapid recovery of the Marine Transportation System (MTS), and continues to actively engage with DHS and industry leaders on this issue.
- Published its Area Maritime Security Plan for south-west Florida and Key West, bringing the total number of such plans to forty-five.
- Continued its joint sponsorship with TSA of the Port Security Training and Exercise Program (PortSTEP). PortSTEP is focused on the development and implementation of a port security inter-modal transportation exercise program for all port and maritime communities to align our national infrastructure protection policies and programs. In 2006, sixteen PortSTEP exercises were conducted in ports nationwide.
- Developed and implemented an Area Maritime Security Training and Exercise Program (AMSTEP) to consolidate and standardize port security exercises, establish specific performance-based measurable objectives, apply a consistent evaluation methodology to those selected objectives, and develop a sustainable multi-year exercise schedule. In 2006, this program exercised forty-two ports to support the MTSA requirement for the updating of Area Maritime Security Plans. This effort also included the development and implementation of a comprehensive Quality Assurance and Surveillance Plan (QASP) that oversees contractor provision of the technical support for AMSTEP exercises.
- Initiated a technical review of the draft Marine Terrorism Response (MTR) Plan - National Model Edition (funded by a DHS grant to the Port Authority of Seattle) to assess the possible use of that plan in supporting MTSA requirements.
- Initiated a comprehensive review of AMSP policy and planning templates, as well as a program of multiple-contingency exercises to recognize MTSA Transportation Security Incident (TSI) issues associated with other hazards. Efforts included conducting combined AMSTEP/PREP exercises in Houston, Texas and Portland, Oregon.
- Expanded its Incident Management procedures for Unified Commands to manage maritime Transportation Security Incidents to reflect the need for continued antiterrorism measures during response and recovery phases of an otherwise non-security incident.
- Co-sponsored with DHS initial stages for ten port-level Underwater Terrorism Prevention Plan (UTPP) workshops

Remaining Plans

- The TWIC Final Rule will be published in early 2007 and will establish how such cards will be issued, how they will be used, and how the Coast Guard will enforce these requirements.
- The Coast Guard will continue to conduct a total of 10 port-level Underwater Terrorism Prevention Plan (UTPP) workshops.
- In 2007, the Coast Guard will conduct thirty-two additional AMSTEP exercises, and nineteen additional PortSTEP exercises.
- The Coast Guard will continue a comprehensive review of Area Maritime Security Plan policy and planning templates and provide expanded planning guidance for facilitating the recovery of the Maritime Transportation System.
- The Coast Guard will continue its technical review of the draft Marine Terrorism Response Plan - National Model Edition to assess its possible use in supporting MTSA requirements.

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 and Intergovernmental Affairs
Chief Financial Officer
Chief Information Officer
Chief Security Officer
Chief Privacy Officer

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) 254-4100, fax your request to (202) 254-4285, 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 the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations - Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528, fax the complaint to (202) 254-4292; or email DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.