THIS FILE IS MADE AVAILABLE THROUGH THE DECLASSIFICATION EFFORTS AND RESEARCH OF:

THE BLACK VAULT

THE BLACK VAULT IS THE LARGEST ONLINE FREEDOM OF INFORMATION ACT / GOVERNMENT RECORD CLEARING HOUSE IN THE WORLD. THE RESEARCH EFFORTS HERE ARE RESPONSIBLE FOR THE DECLASSIFICATION OF THOUSANDS OF DOCUMENTS THROUGHOUT THE U.S. GOVERNMENT, AND ALL CAN BE DOWNLOADED BY VISITING:

HTTP://WWW.BLACKVAULT.COM

YOU ARE ENCOURAGED TO FORWARD THIS DOCUMENT TO YOUR FRIENDS, BUT PLEASE KEEP THIS IDENTIFYING IMAGE AT THE TOP OF THE .PDF SO OTHERS CAN DOWNLOAD MORE!

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

SEMIANNUAL REPORT TO THE CONGRESS

October 1, 2006 – March 31, 2007

Working Relationship Principles For Agencies and Offices of Inspector General

The *Inspector General Act* establishes for most agencies an Office of Inspector General (OIG) and sets out its mission, responsibilities, and authority. The Inspector General is under the general supervision of the agency head. The unique nature of the Inspector General function can present a number of challenges for establishing and maintaining effective working relationships. The following working relationship principles provide some guidance for agencies and OIGs.

To work most effectively together, the Agency and its OIG need to clearly define what the two consider to be a productive relationship and then consciously manage toward that goal in an atmosphere of mutual respect.

By providing objective information to promote government management, decision-making, and accountability, the OIG contributes to the Agency's success. The OIG is an agent of positive change, focusing on eliminating waste, fraud, and abuse, and on identifying problems and recommendations for corrective actions by agency leadership. The OIG provides the agency and Congress with objective assessments of opportunities to be more successful. The OIG, although not under the direct supervision of senior agency management, must keep them and the Congress fully and currently informed of significant OIG activities. Given the complexity of management and policy issues, the OIG and the Agency may sometimes disagree on the extent of a problem and the need for and scope of corrective action. However, such disagreements should not cause the relationship between the OIG and the Agency to become unproductive.

To work together most effectively, the OIG and the Agency should strive to:

Foster open communications at all levels. The Agency will promptly respond to the OIG requests for information to facilitate OIG activities and acknowledge challenges that the OIG can help address. Surprises are to be avoided. With very limited exceptions primarily related to investigations, the OIG should keep the Agency advised of its work and its findings on a timely basis, and strive to provide information helpful to the Agency at the earliest possible stage.

Interact with professionalism and mutual respect. Each party should always act in good faith and presume the same from the other. Both parties share as a common goal–the successful accomplishment of the Agency's mission.

Recognize and respect the mission and priorities of the Agency and the OIG. The Agency should recognize the OIG's independent role in carrying out its mission within the Agency, while recognizing the responsibility of the OIG to report both to the Congress and to the Agency Head. The OIG should work to carry out its functions with a minimum of disruption to the primary work of the Agency.

Be thorough, objective, and fair. The OIG must perform its work thoroughly, objectively, and with consideration to the Agency's point of view. When responding, the Agency will objectively consider differing opinions and means of improving operations. Both sides will recognize successes in addressing management challenges.

Be engaged. The OIG and Agency management will work cooperatively in identifying the most important areas for OIG work, as well as the best means of addressing the results of that work, while maintaining the OIG's statutory independence of operation. In addition, agencies need to recognize that the OIG also will need to carry out work that is self-initiated, congressionally requested, or mandated by law.

Be knowledgeable. The OIG will continually strive to keep abreast of agency programs and operations, and Agency management will be kept informed of OIG activities and concerns being raised in the course of OIG work. Agencies will help ensure that the OIG is kept up to date on current matters and events.

Provide feedback. The Agency and the OIG should implement mechanisms, both formal and informal, to ensure prompt and regular feedback.

Photo Credits, Cover Page: U.S. Customs and Border Protection Photo Library. Border Patrol Agents in a fast rope exercise, CBP Officers undergoing training, and U.S. Coast Guard Photo Library.

Office of Inspector General

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

Homeland Security

April 30, 2007

The Honorable Michael Chertoff
Secretary
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Mr. Secretary:

I am pleased to present our semiannual report, which summarizes the activities and accomplishments of the Department of Homeland Security (DHS) Office of Inspector General for the 6-month period ending March 31, 2007.

For the first time, we present scorecards depicting the progress the department has made in addressing major management challenges in its acquisition programs. We surveyed select DHS acquisition functions and activities to determine the efficacy of those operations. The scorecards focus on acquisition operations in DHS as a whole and at the Federal Emergency Management Agency. We also assessed the acquisition activities of the United States Coast Guard's Integrated Deepwater System Program (Deepwater) and Customs and Border Protection's Secure Border Initiative network Program (SBInet).

During this reporting period, our office issued 36 management reports and 16 financial assistance grant reports. In addition, we processed 106 reports on DHS programs that were issued by other organizations. As a result of these efforts, $53 million of questioned costs were identified, of which $6 million were determined to be unsupported. In addition, we identified $1.3 million of funds that could be put to better use. I am most satisfied, however, with the positive response our reports have received from departmental management. Departmental managers have concurred with approximately 97% of our recommendations.

In the investigative area, we issued 341 reports. Our investigations resulted in 286 arrests, 245 indictments, 121 convictions, and 18 personnel actions. Our investigators closed 367 investigations. We received 8,619 complaints. Of these complaints, we referred 4,989 complaints to departmental components for action, and closed approximately 8,592 complaints, or 99.7%. Additionally, investigative recoveries, fines, restitutions, and cost savings totaled $8.3 million.

As we close this reporting period, the department faces the unprecedented challenge of continuing to focus on its mission, while coordinating recovery efforts in the wake of Hurricane Katrina, the costliest natural disaster in our Nation's history. Our office will continue to work with and assist DHS program managers in ensuring that the billions of dollars targeted to support the recovery and reconstruction effort are spent wisely and in the most effective manner possible.

In closing, I would like to thank all of the hardworking and dedicated professionals in the DHS Office of Inspector General. As a result of their efforts, we were able to successfully meet the tremendous challenges that faced our office during the past 6 months. Their selfless dedication to service, oftentimes at the expense of time with family and friends, has not gone unnoticed and is truly commendable.

I also would like to take this opportunity to thank you for the interest and support that you have provided to our office to date. We look forward to working closely with you, your leadership team, and the Congress toward the goal of promoting economy, efficiency, and effectiveness in DHS programs and operations, as well as helping the department accomplish its critical mission in the very challenging months ahead.

Sincerely,

Richard L. Skinner
Inspector General

TABLE OF CONTENTS

STATISTICAL HIGHLIGHTS OF OIG ACTIVITIES
October 1, 2006 – March 31, 2007

Dollar Impact

Questioned Costs	$53,328,190
Funds Put to Better Use	$1,329,074
Management Agreement That Funds Be:	
Recovered	$0
De-obligated	$860,000
Funds Recovered (Audits)	$188,990
Fines and Restitutions	$3,845,747
Administrative Cost Savings and Investigative Recoveries	$4,434,607

Activities

Management Reports Issued	36
Financial Assistance Grant Audit Reports	16
Investigation Reports Issued	341
Single Audit Reports Processed	57
Defense Contract Audit Agency	49
Investigations Initiated	516
Investigations Closed	367
Open Investigations	2,725
Investigations Referred for Prosecution	118
Investigations Accepted for Prosecution	173
Investigations Declined for Prosecution	40
Arrests	286
Indictments	245
Convictions	121
Personnel Actions	18
Complaints Received (other than Hotline)	4,512
Hotline Complaints Received	4,107
Complaints Referred (to programs or other agencies)	4,989
Complaints Closed	8,592

EXECUTIVE SUMMARY

This is the ninth semiannual report to Congress issued by the Department of Homeland Security (DHS) Office of Inspector General since its establishment in January 2003. It is issued pursuant to the provisions of Section 5 of the *Inspector General Act of 1978*, as amended, and covers the period from October 1, 2006, to March 31, 2007. The report is organized to reflect our organization and that of DHS.

We have published scorecards identifying the progress made in selected acquisition functions and activities within the DHS. The scorecards summarize the progress of previously issued audits and inspections, supplemented by additional fieldwork. They focus on acquisition operations in DHS as a whole and at the Federal Emergency Management Agency. We also assessed the United States Coast Guard's Integrated Deepwater System Program and the United States Customs and Border Protection's Secure Border Initiative Program.

During this reporting period, we completed significant audit, inspection, and investigative work to promote the economy, efficiency, effectiveness, and integrity of DHS programs and operations. Specifically, we issued 36 management reports (Appendix 3), 16 financial assistance grant reports (Appendix 4), and 341 investigative reports. We also processed 106 reports on DHS programs: 49 audits issued by the Defense Contract Audit Agency and 57 single audits issued by other organizations according to the *Single Audit Act of 1984,* as amended (Appendix 4). Our reports provide the DHS Secretary and Congress with an objective assessment of the issues, while at the same time providing specific recommendations to correct deficiencies and improve the economy, efficiency, and effectiveness of the respective program.

During this reporting period our audits resulted in questioned costs of $53,328,190 of which $6,168,625 was determined to be unsupported costs. In addition, we identified $1,329,074 of funds that could be put to better use. We also recovered $188,990 as a result of disallowed costs identified from two prior audits. Our investigations resulted in 286 arrests, 245 indictments, and 121 convictions. Moreover our investigators closed 367 investigations and 8,592 complaints. Additionally, investigative recoveries, restitutions, fines, and cost savings totaled $8,280,354.

We have a dual reporting responsibility to Congress as well as to the Secretary. During the reporting period, we continued our active engagement with Congress through numerous meetings, briefings, and dialogues with members and staff of the department's authorizing and appropriations committees and subcommittees on a range of issues relating to our work and that of the DHS. We also testified before Congress on eight occasions during this reporting period. Testimony prepared for these hearings may be accessed through our website at www.dhs.gov/oig.

DEPARTMENT OF HOMELAND SECURITY PROFILE

On November 25, 2002, President Bush signed the *Homeland Security Act* (PL 107-296, as amended), officially establishing the Department of Homeland Security (DHS) with the primary mission of protecting the American homeland. On January 24, 2003, DHS became operational. Formulation of DHS took a major step forward on March 1, 2003, when, according to the President's reorganization plan, 22 agencies and approximately 181,000 employees were transferred to the new department.

DHS' first priority is to protect the Nation against further terrorist attacks. Component agencies analyze threats and intelligence, guard U.S. borders and airports, protect America's critical infrastructure, and coordinate U.S. preparedness for and response to national emergencies.

DHS has been reorganized into the following directorates:

Management
National Protection and Programs
Science and Technology

Other critical components of DHS include:

Domestic Nuclear Detection Office
Federal Emergency Management Agency
Federal Law Enforcement Training Center
Office of Civil Rights and Civil Liberties
Office of Health Affairs
Office of Intelligence and Analysis
Office of Operations Coordination
Office of Policy
Transportation Security Administration
United States Citizenship and Immigration Services
United States Coast Guard
United States Customs and Border Protection
United States Immigration and Customs Enforcement
United States Secret Service

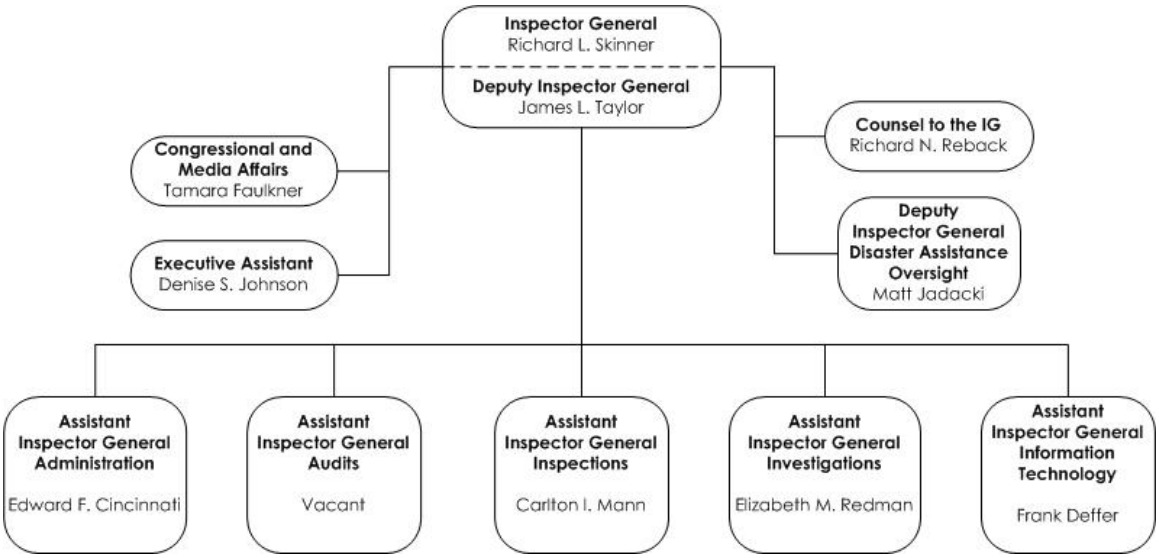
OFFICE OF INSPECTOR GENERAL PROFILE

The *Homeland Security Act of 2002* provided for the establishment of an Office of Inspector General (OIG) in DHS by amendment to the *Inspector General Act of 1978* (5 USC App. 3, as amended). By this action, Congress and the administration ensured independent and objective audits, inspections, and investigations of the operations of the department.

The Inspector General is appointed by the President, subject to confirmation by the Senate, and reports directly to the Secretary of DHS and to Congress. The *Inspector General Act* ensures the Inspector General's independence. This independence enhances our ability to prevent and detect fraud, waste, and abuse as well as to provide objective and credible reports to the Secretary and Congress regarding the economy, efficiency, and effectiveness of DHS' programs and operations.

We are authorized to have 545 full-time employees. We currently have approximately 166 permanent and temporary employees providing audit and investigative efforts to our Office of Disaster Assistance Oversight operations. We are composed of five functional components and are based in the District of Columbia. We have 22 permanent field offices throughout the country and seven temporary field offices dedicated to our disaster oversight operations. The following organization chart illustrates our Management Team.

Chart 1: DHS OIG Organization Chart



SUMMARY OF SIGNIFICANT OIG ACTIVITY

DIRECTORATE FOR MANAGEMENT

MANAGEMENT REPORTS

Independent Auditors' Report on DHS' Fiscal Year 2006 Financial Statements (Excerpts from the DHS Performance and Accountability Report)

The independent public accounting firm KPMG prepared the independent auditors' report on DHS' financial statements. KPMG concluded that the department made some progress at the component level to improve financial reporting during FY 2006, although overall it still has much work remaining. For the third year, KPMG was unable to provide an opinion on the department's balance sheet, and the number of material weaknesses remains at ten.

In FY 2006, the department gained new leadership in financial management with the confirmation of a presidentially appointed Chief Financial Officer. However, the department continued to struggle with financial reporting during FY 2006. The Office of Financial Management, Coast Guard, Transportation Security Administration (TSA), Federal Emergency Management Agency (FEMA), Immigration and Customs Enforcement (ICE), and Management Directorate were unable to provide sufficient evidence to support account balances presented in the financial statements and collectively contributed to the auditors' inability to render an opinion. Further, DHS management and three of its major components [United States Coast Guard (USCG), TSA, and ICE] were unable to represent that the financial statements were presented in conformity with U.S. generally accepted accounting principles.

At the component level, there was some progress in addressing internal control weaknesses. ICE achieved the greatest improvement in financial management and reporting in FY 2006. Contributing to ten material weaknesses in FY 2005, it contributed to only one material weakness in FY 2006. ICE mitigated the severity of its material weaknesses through corrective actions implemented during 2006, but has not completely resolved its internal control problems.

The USCG began FY 2006 with a focus on financial management oversight, financial reporting, and fund balance with Treasury. Unfortunately, progress has been slow and the auditors again reported that the USCG did not have an organizational structure that fully supported the development and implementation of effective policies, procedures, and internal controls. Management officials within USCG acknowledged to the auditors that longstanding procedural, control, personnel, and cultural issues existed and had

impeded their progress in installing an effective financial management structure. The auditors reported that the USCG's personnel rotation policy, among other issues, made it difficult for USCG's Chief Financial Officer to institutionalize internal controls related to financial management and reporting.

Many of the department's difficulties in financial management and reporting can be attributed to the original stand-up of a large, new, and complex executive branch agency without adequate organizational expertise in financial management and accounting. The department has recently committed to obtaining additional human resources and other critical infrastructure necessary to develop reliable financial processes, policies, procedures, and internal controls that will enable management to represent that financial statements are complete and accurate. These resources and infrastructure are critical to the implementation of effective corrective actions and to establish an effective financial management oversight function. During the past year, the department and its components began an extensive effort to develop meaningful corrective action plans to address specific material internal control weaknesses.

The auditors reported the following ten material weaknesses: financial management and oversight; financial reporting; financial systems security; fund balance with Treasury; property, plant, and equipment; operating materials and supplies; legal and other liabilities; actuarial liabilities; budgetary accounting; and intragovernmental balances. The auditors reported two other notable conditions: environmental liabilities and custodial revenue and drawback.

The auditors reported that DHS and each significant component did not fully comply with at least one of the requirements of the *Federal Financial Management Improvement Act*. Noncompliance is due to the material weaknesses and reportable conditions cited above, and corrective action plans must be developed to address those weaknesses and conditions. (OIG-07-10, November 2006, OA)

DHS' Corrective Action Plan Process for Financial Reporting - Report No. 3

KPMG performed an audit of DHS' corrective action plans developed to address five of the ten material weaknesses in internal control cited in the Independent Auditor's Report included in the department's FY 2005 Performance and Accountability Report. The five material weaknesses are: property, plant, and equipment; operating materials and supplies; undelivered orders, accounts and grants payable, and disbursements; budgetary accounting; and intragovernmental and intradepartmental balances. These weaknesses are primarily attributable to five entities within DHS: Office of the Chief Financial Officer, USCG, ICE, TSA, and Grants and Training[1]. (OIG-07-13, December 2007, OA)

[1] The Office of Grants and Training, formerly under the Directorate for Preparedness, recently moved to the new FEMA and was renamed the "Office of Grant Programs."

DHS' Corrective Action Plan Process for Financial Reporting - Report No. 4

We conducted a review of DHS' corrective action plan process for financial reporting to (1) assess the integrity of the corrective action plans, updated as of September 30, 2006, related to 4 of the 10 material weaknesses that were cited in the independent auditors' report; (2) evaluate the alignment of 5 contracts awarded to support actions to correct specific material weaknesses; and (3) evaluate the Financial Management Transformation and Chief Financial Officer Audit Remediation task force activities taken in response to the Commandant's Order issued July 3, 2006.

We identified weaknesses in the initial root cause exercise that was performed to draft the corrective action plans. For the plans reviewed, it remains difficult to determine if all conditions of the material weaknesses have been identified and whether the root causes that have been identified are adequate to assist management with developing effective remediation plans. Also, USCG management did not consider business risks, materiality, or cost versus benefit analysis when developing the remediation plans. The plans include high-level work breakdown structures but not resource estimates for each subtask of the milestones or a formal process for reporting progress against each Corrective Action Plan's milestones. For the four plans, accountability for all areas, including accountability below the process owner level, has not been fully determined. In addition, USCG has not defined procedures to assess the effectiveness of its remediation activities.

We recommended that USCG (1) validate the existing corrective action plans root cause analysis; (2) develop crosswalks to ensure all conditions leading to identified material weaknesses are tracked to the root causes; (3) update the current work breakdown structures for the remediation plans after the root cause analysis and validation efforts are completed; (4) develop a risk-based plan for each of the four corrective action plans to prioritize tasks and assist with aligning resources to high-value tasks; and (5) designate a USCG owner or senior-level executive responsible for the coordination of all financial management and reporting improvement initiatives. (OIG-07-29, February 2007, OA)

DHS' Internal Control Over Financial Reporting – FY 2006

We reviewed the effectiveness of DHS' internal control over financial reporting as of September 30, 2006, based on the criteria established under the Federal Managers' Financial Integrity Act. We determined that DHS did not maintain effective internal controls over financial reporting based on the ten material weaknesses that were reported by DHS' independent auditor. (OIG-07-20, December 2006, OA)

DHS' Implementation of Protective Measures for Personally Identifiable Information

We reviewed the DHS' implementation of the recommendations set forth in the Office of Management and Budget (OMB) Memorandum 06-16, *Protection of Sensitive Agency*

Information. Our objective was to determine whether DHS has effectively implemented safeguards to protect sensitive and personally identifiable information (PII).

DHS and its components are in the process of implementing OMB's recommended security controls for sensitive data and PII. DHS has issued updated policies and procedures to address OMB's recommendations. Further, DHS is in the process of identifying PII systems, encrypting laptop computers, and implementing remote access security and offsite transportation and storage controls. Until all systems collecting, processing, or storing PII are identified, and proper controls for protecting remote access and storage of PII are implemented, DHS does not have assurance that sensitive data are properly protected.

We recommended that the Chief Privacy Officer ensure completion of the identification of systems that collect, process, or store PII, as well as the assessment of the risk associated with the systems and data. In addition, we recommended that the Chief Information Officer: (1) encrypt PII stored on laptop computers and mobile computing devices, as well as data transported and stored at an alternate facility; (2) establish proper remote access security controls for access to PII, including two-factor authentication for remote access connections and session termination after 20 minutes of inactivity; (3) implement sufficient controls over copies and extracts of PII, including procedures to ensure that copies or extracts made by users or administrators are erased within 90 days if no longer required; and (4) identify aspects of the updated DHS policies and procedures requiring clarification, and provide additional guidance to component officials on the requirements. DHS concurred with the recommendations and plans to take steps to implement each of the recommendations. (OIG-07-24, January 2007, IT)

DIRECTORATE FOR NATIONAL PROTECTION AND PROGRAMS

MANAGEMENT REPORTS

The Department of Homeland Security's Role in Food Defense and Critical Infrastructure Protection

The federal government is charged with defending the food supply from intentional attacks and natural hazards. While DHS is not the designated lead for a number of key activities in this area, Congress and the President have assigned DHS many important food defense and critical infrastructure protection responsibilities. This report examines DHS activities relating to post-harvest food, and focuses on prevention, protection, preparedness, and detection efforts.

We observed four main limitations in DHS' related efforts.

- First, DHS could improve internal coordination of its related efforts. DHS food sector activities are distributed across multiple organizational units, and similar program thrusts have emerged. Consolidated management attention is required to reduce the risk of duplication and promote collaboration.
- Second, DHS needs to improve its engagement of public and private food sector partners. Food sector partners were frustrated by the quality and extent of DHS external coordination in sector governance and information sharing; mapping; and research, development, education, and training.
- Third, DHS could do more to prioritize resources and activities based on risk. DHS units have used different approaches to prioritizing food sector activities in the context of their larger missions and have not developed a common perspective on food sector risk.
- Finally, DHS must fully discharge its food sector responsibilities. DHS has satisfied basic requirements in most, but not all, areas of responsibility. The department has not submitted an integrated federal food defense budget plan or clearly established assessment standards for use in the food sector.

Our report contains 16 recommendations to enhance DHS' performance and improve the security posture of the food supply. DHS concurred with 12 of these recommendations. (OIG-07-33, February 2007, ISP)

DIRECTORATE FOR SCIENCE AND TECHNOLOGY

MANAGEMENT REPORTS

DHS' Management of BioWatch Program

DHS, through the Science and Technology Directorate, provides management oversight to the BioWatch program (BioWatch), an early warning system designed to detect the release of biological agents in the air through a comprehensive protocol of monitoring and laboratory analysis. We conducted a review of BioWatch to determine the extent BioWatch program management implemented proper controls for coordinating responsibilities and funding with its partner agencies.

The program operates in various cities, but DHS still needs to design and implement management controls to follow up on deficiencies in field and laboratory operations. Further, DHS has not properly enforced or monitored partner agency reporting needed to coordinate BioWatch. The need to enhance management controls over BioWatch exposes

the program to possible mismanagement of funds and could jeopardize DHS' ability to detect biological agents and protect the populace of the United States.

We recommended that the Under Secretary for Science and Technology: (1) address and rectify after-action and previous field operation findings; (2) enforce Federal partners' requirements, including monthly and quarterly reporting requirements; and (3) closely review and monitor required reports submitted by its Federal partners to determine and resolve discrepancies. (OIG-07-22, January 2007, OA)

FEDERAL EMERGENCY MANAGEMENT AGENCY

MANAGEMENT REPORTS

Management Advisory Report on Condition, Losses, and Possible Uses of FEMA Modular Housing

Modular homes are factory-built in sections and transported to a building site, where the sections are joined together to form a residential unit that can be used to shelter disaster evacuees. As part of our oversight responsibilities regarding FEMA's management of modular homes that were purchased in the wake of Hurricane Katrina but never used, we revisited the emergency housing sites at Texarkana, Texas, and Hope, Arkansas, where more than 1,000 modular homes are stored. Our objectives were to assess whether FEMA correctly implemented our February 2006 recommendations to ensure that the units were properly stored and maintained to mitigate deterioration, and that damaged units were repaired.

Most of the modular homes were not properly stored and have been significantly damaged. Based on an evaluation by representatives of the homes' manufacturers, we estimate that the cost of the damage is several million dollars.

FEMA has agreed to implement our recommendations, which include: (1) inventory and determine the extent of damage to all modular home units currently in stock; (2) formally write off all modular home units that are beyond economical repair; (3) make cost-effective plans for the use of all remaining modular home units; (4) protect and maintain all those modular home units whose condition merits retention; and (5) develop written policies and procedures that allow the purchase of modular home units only when the requirement has been clearly identified, and ensure that they are packaged satisfactorily for storage and are properly stored. (OIG-07-03, October 2006, DAO)

FEMA's Progress in Addressing Information Technology Management Weaknesses

FEMA is responsible for coordinating disaster relief efforts across federal, state, and volunteer organizations, such as the American Red Cross. FEMA relies heavily on information technology (IT) systems to carry out its response and recovery operations. Strategic management of these assets is important to ensure that the technology can perform effectively during times of disaster and tremendous stress.

We conducted a follow up audit to determine the status of FEMA's efforts to address the response and recovery technology weaknesses detailed in our September 2005 audit report, *Emergency Preparedness and Response Could Better Integrate Information Technology With Incident Response and Recovery* (OIG-05-36). In the report, we reviewed FEMA's approach to responding to and recovering from terrorist attacks, major disasters, and other domestic emergencies; assessed the effectiveness of guidance and processes to support IT users during incident management; and determined and evaluated existing and proposed systems and other technologies to help carry out FEMA's mission. For this followup audit, we evaluated the progress that FEMA has made to address our prior report recommendations within the context of its plans and activities to improve the National Emergency Management Information System (NEMIS). We examined FEMA's IT improvement efforts in both the short-term as the agency prepared for the 2006 hurricane season, as well as in the long-term as it works to align with the department's overarching strategic direction.

FEMA has made progress in several areas, particularly short-term adjustments to prepare for the 2006 hurricane season. These improvements primarily included increasing NEMIS capacity and online system access and strengthening verification of registration data. In addition, FEMA and its program offices specifically addressed our recommendations by documenting training resources, developing a plan to implement its enterprise architecture, gathering requirements for new business tools, and improving configuration management.

However, despite these positive steps, FEMA has not documented or communicated a strategic direction to guide long-term IT investment and system development efforts. FEMA also has not performed crosscutting requirement gathering to determine business needs, which would allow Information Technology Services Division personnel to analyze alternatives to continued development of the complex, custom NEMIS system. In addition, FEMA has several resource challenges to accomplishing these tasks, including personnel needs, time limitations, and funding constraints. Therefore, constrained by limited resources, FEMA focused its efforts on preparation for the 2006 hurricane season and has made little progress in addressing long-term needs, such as updating strategic plans, defining cross-cutting requirements, and evaluating systems alternatives. (OIG-07-17, December 2006, IT)

Special Transient Accommodations Program for the Evacuees From Hurricanes Katrina and Rita

After Hurricanes Katrina and Rita with their unprecedented damage and displacement of residents, FEMA entered into contracts with the American Red Cross and Corporate Lodging Consultants (the Consultants) to provide temporary housing for evacuees. We contracted with the firm of Ollie Green & Company, CPAs, to review whether FEMA, through the American Red Cross and the Consultants, effectively implemented a plan that would properly determine: (1) evacuee eligibility for lodging; (2) allowableness of charges; (3) reasonableness of room rates; and (4) compliance with Federal Acquisition Regulations.

American Red Cross and the Consultants did not always follow procedures authorized by FEMA for determining evacuee eligibility or require hotels and motels to follow standard industry protocols. Billed room rates were greater than published rates. Definitive proof of occupancy prior to authorizing payments was not required. From our judgmental sample of 3,000 evacuees, we questioned costs of $3.4 million.
(OIG-07-31, February 2007, DAO)

FEMA's Award of 36 Trailer Maintenance and Deactivation Contracts

At the request of Senators Byron L. Dorgan and Mary L. Landrieu, we reviewed FEMA's award of 36 contracts worth $3.6 billion for the maintenance and deactivation of travel trailers and manufactured housing needed after hurricanes Katrina and Rita. The Senators' letter asked us to investigate the bid process and address concerns raised by witnesses who testified before the Senate Democratic Policy Committee on May 19, 2006.

Overall, FEMA contracting officials treated bidders fairly during the bid process. However, to fully realize the goal of maximizing local participation, they should have established better criteria for determining whether a bidder was a local firm. FEMA officials did not design the solicitation to maximize preference to local businesses. They also should have analyzed prices more thoroughly before awarding the contracts to ensure that costs were reasonable. Contracting officials also did not properly assess the wide range of prices proposed by bidders and thereby exposed FEMA to both the risk of paying too much for contract line items as well as not paying enough to ensure proper performance. Finally, FEMA officials did not provide unsuccessful bidders with line-item prices, as required during post award debriefings.

We recommended that FEMA's Chief Procurement Officer issue guidance to contracting staff to: 1) Emphasize the importance of assessing price reasonableness and price realism before awarding contracts; 2) Develop written guidance for the implementation of the new statutory provision and interim rule to ensure FEMA contracting officers properly

determine whether a business is local (FAR Subpart 26.2); and 3) Reinforce the FAR requirement to disclose unit prices as part of post award debriefings.
(OIG-07-36, March 2007, DAO)

The State of North Carolina's Management of State Homeland Security Grants Awarded During Fiscal Years 2002 and 2003 FY 2006

The Office for Domestic Preparedness[2] awarded about $58 million to the State of North Carolina from the FY 2002 State Domestic Preparedness Program, and from Parts I and II of the FY 2003 State Homeland Security Grant Program. McBride, Lock & Associates, under a contract with our office, conducted the audit to determine whether North Carolina: (1) effectively and efficiently implemented the first responder grant programs, (2) achieved the goals of the programs, and (3) spent funds according to grant requirements.

While North Carolina attempted to conscientiously manage the first responder grant programs, it did not measure accountability in achievement of the Office for Domestic Preparedness-approved strategic plan. Frequent changes in the grantee's management team adversely affected the state's management of the programs. Additionally, the need for written policies and procedures and the inadequacy of the budget structure diminished the effectiveness of the administration of the programs. The need to hire through temporary employment agencies also caused security concerns because of the sensitive nature of information that they may have processed. The state made some payments for unnecessary equipment and other unsupported purchases and did not always properly monitor subgrantees. We reported delays in the expenditure of grant funds as well as limitations on measurement standards to determine the effectiveness or efficiency of North Carolina's progress in preparing for terrorist incidents.
(OIG-07-02 October 2006, OA)

Emergency Management Performance Grant Funds Awarded to the Virgin Islands Territorial Emergency Management Agency

We audited Emergency Management Performance Grant (EMPG) funds awarded to the Virgin Islands Territorial Emergency Management Agency (VITEMA). The objective of the audit was to determine whether VITEMA accounted for and expended grant funds in compliance with financial and program regulations.

VITEMA received three EMPG awards totaling $1,868,296 from FEMA. Our audit covered the grant period October 2001 to June 2005, during which VITEMA expended

[2] The Office for Domestic Preparedness was part of the former Directorate for Preparedness and had been renamed the Office of Grants and Training. The Office of Grants and Training recently moved to the new FEMA and was renamed the "Office of Grant Programs."

$1,800,186 and drew down $1,868,296 of FY 2002, 2003 and 2004 EMPG funds. We reviewed the appropriateness of $558,703 of these expenditures.

VITEMA did not expend and account for all EMPG funds according to federal regulations and EMPG guidance. We questioned $190,877 of costs claimed by VITEMA because they improperly allocated personnel costs totaling $188,969, and professional service charges totaling $1,908 to the grant. VITEMA did not follow required cash management procedures when receiving and disbursing federal funds.

The audit determined that VITEMA charged $188,969 to EMPG for personnel costs that should have been allocated to other activities. For costs to be allocable, the U.S. Office of Management and Budget Circular A-87, Cost Principles for State, Local and Indian Tribal Governments, states that a cost is allocable to a particular cost objective if the goods or services involved are chargeable or assignable to such cost objective in accordance with relative benefits received. VITEMA charged 100 percent of the salaries of three employees to EMPG. However, these employees did not spend 100 percent of their time on EMPG activities. In addition, we questioned the $1,908 of professional service charges that should have been allocated to another program.

We recommended that the Regional Director, FEMA Region II disallow the $190,877 of questioned costs unallocable to EMPG pending Region II's final determination about the eligibility of the VITEMA salary costs allocated to the grant; require VITEMA to submit supporting documentation that clearly identifies the Pre-Disaster Mitigation activities that benefit EMPG; and ensure that VITEMA more accurately accounts for and charges staff time to its various grant programs in the future. (DA-07-01, October 2006, OA)

GRANT REPORTS

We issued 16 financial assistance grant reports. The majority of the reports related to presidentially declared disasters. We questioned costs totaling $23,046,371 of which $2,083,300 was unsupported. In addition, we identified $860,000 in funds put to better use. An itemized list of these reports, including questioned costs, unsupported costs, and funds put to better use, is provided in Appendix 4.

Hurricane Wilma Activities for the City of Port Saint Lucie, Florida, FEMA Disaster 1609-DR-FL

The City of Port Saint Lucie (City) received an award of $4.0 million from the Florida Department of Community Affairs, a FEMA grantee, for emergency protective measures and debris removal activities associated with Hurricane Wilma. We performed an interim review of costs incurred under the award to determine whether the City properly accounted for disaster-related costs and whether such costs were eligible for funding under FEMA's public assistance program; and also whether the City awarded contracts

according to federal procurement standards and had adequate procedures for monitoring the activities of its contractors.

The City needs an effective system for accounting for disaster-related costs and did not comply with federal procurement standards when contracting for debris removal monitoring services. Moreover, the City's project expenditures contained $623,459 of costs that were ineligible for FEMA funding. These costs included $447,116 of regular-time salaries for permanent City employees who performed emergency services work and $176,343 of costs associated with removing debris from federal-aid roads, which are the responsibility of the Federal Highway Administration.

We recommended that the Director of FEMA's Florida Long-Term Recovery Office, in conjunction with the grantee, (1) instruct the City, for future declarations, to establish and maintain separate accountability for expenditures under each FEMA project, and to comply with federal procurement regulations when awarding contracts for FEMA-funded activities, (2) disallow $447,116 of regular-time salary costs related to emergency work, and (3) inform the City that it should remove the previously disallowed debris removal costs of $176,343 associated with federal-aid roads from FEMA project expenditures. (DA-07-04, November 2006, DAO)

Hurricane Wilma Activities for the City of Coral Gables, Florida

The City of Coral Gables (City) received an award of $14.3 million from the Florida Department of Community Affairs, a FEMA grantee, for emergency protective measures and debris removal associated with Hurricane Wilma. We performed an interim review of costs incurred under the award to determine whether the City was properly accounting for disaster-related costs and whether such costs were eligible for funding under FEMA's public assistance program.

The City had an effective system for accounting for disaster-related costs and the City's contracts for debris removal activities were awarded according to federal procurement regulations. However, the City's claim included $365,633 of excessive equipment costs resulting from idle equipment time. FEMA guidelines state that equipment rates are applied only to the time the equipment is actually working, and that standby time and idle time are not eligible.

We recommended that the Director of FEMA's Florida Long-Term Recovery Office, in conjunction with the grantee, disallow the $365,633 of excessive equipment costs. (DA-07-06, December 2006, DAO)

University of Texas Health Science Center, Houston, Texas

We audited public assistance funds awarded to the University of Texas Health Science Center (Center), Houston, Texas. Our audit objective was to determine whether the Center accounted for and expended FEMA funds according to federal regulations and FEMA guidelines. The Center received an award of $39.4 million from the Texas Governor's Division of Emergency Management, a FEMA grantee, for damages caused by Tropical Storm Allison in June 2001.

The Center did not account for and expend all FEMA funds according to federal regulations and FEMA guidelines. The Center's claim included $1,903,825 (FEMA share $1,427,869) in questioned costs, consisting of $1,268,303 in ineligible contractor costs and $635,522 in unsupported contractor costs. In addition, the Center did not follow all federal procurement standards or FEMA guidelines in awarding contracts totaling $14,553,491. However, we did not question costs based solely on noncompliance with federal procurement standards because the procurements occurred under exigent circumstances. (DD-07-01, October 2006, DAO)

St. Bernard Parish Louisiana's Management of Department of Homeland Security Grants Awarded for Removal of Debris from Hurricane Katrina

Foxx & Company performed this audit for our office. The objective of the review was to determine whether the awarded contracts and contractor billings were in compliance with applicable Federal criteria. Foxx also reviewed selected aspects of the overall management of debris removal and monitoring within the Parish because of the magnitude of the devastation, the volume of debris created by Hurricane Katrina, and the length of time that it would take to complete the removal process. The scope of the review included all debris removal and monitoring activities managed by St. Bernard Parish during the period August 29, 2005, to March 31, 2006.

FEMA estimated that about 5.3 million cubic yards of residential debris was created within the Parish as a result of Hurricane Katrina. Although commendable progress had been made to clean up the Parish, a huge amount of debris remained. As of March 31, 2006, about 4 million cubic yards of debris still needed to be removed.

The Parish awarded a noncompetitive contract for debris removal without performing the required cost and pricing analysis. Foxx questioned $209,115 in ineligible costs for pruning of hanging tree branches and $84,600 for unreasonable or duplicative costs claimed under the monitoring contract. Foxx also pointed out opportunities for improved controls over load ticket processing and improved accuracy during the debris hauling process, and recommended that FEMA switch to using actual weight for debris hauled versus the current method of estimating amounts by volume (tons versus cubic yards).

We recommended that FEMA determine if adjustments should be made to St. Bernard Parish invoices and disallow costs determined to be ineligible or unallowable. We further recommended that FEMA review current and future costs to ensure that hourly rates are fair and equitable and that time claimed is directly in support of debris monitoring activities. (DD-07-02, November 2006, DAO)

Landfill Cost Issues Relating to Disposal of Debris in the City of New Orleans

At the request of a member of Congress, we reviewed issues related to landfill costs for debris disposal in the City of New Orleans, Louisiana (City). The objectives were: to determine whether waste deposited at the Chef Menteur Landfill was from U.S. Army Corps of Engineers (Corps) contracts funded by FEMA; to examine an agreement for the landfill operator to "donate" a percentage of revenues to the City; to determine whether Chef Menteur was the most cost-effective landfill in the region; and to determine whether this was a link between the creation of Chef Menteur, the "donations" from the landfill operator to the City, and the high tipping fees (disposal charges by the landfill operator).

The donation agreement was not appropriate because the "donations" agreed to by the Chef Menteur landfill operator and the mayor of the City increased debris removal costs without justification or added benefits. In substance, the donations should be treated as a credit and deducted from the City's final claim to reduce FEMA's cost of debris removal. Even with the added cost of the donations, the Corps' landfill use of Chef Menteur was more cost effective and productive than the use of Highway 90 Landfill, but using the Gentilly Landfill was more cost effective and productive than using either Chef Menteur or Highway 90. However, FEMA severely restricted the use of the Gentilly Landfill by limiting it to 5,000 cubic yards of debris per day. In addition, the August 15, 2006, closure of Chef Menteur resulted in higher costs and slower debris removal.

We recommended that the Director of FEMA's Louisiana Transitional Recovery Office require the City to treat its receipts under the donation agreement, currently estimated at $860,000, as a credit to be deducted from the City's claim for other disaster costs. FEMA officials agreed. (DD-07-03, December 2006, DAO)

City of Houston, Houston, Texas

We audited $16.04 million in FEMA public assistance funds awarded to the City of Houston (City). The City received the award for damages resulting from Tropical Storm Allison, which occurred on June 5, 2001.

The City did not expend and account for all FEMA funds according to federal regulations and FEMA guidelines. Consequently, we questioned $2,737,128 ($2,052,846 FEMA share) in claimed costs that were unsupported, ineligible, or duplicated, and recommended that FEMA Regional Director, Region VI, disallow the costs. (DD-07-04, January 2007, DAO)

Hurricane Katrina Activities, Plaguemines Parish Sheriff's Office, Louisiana

We performed an interim review of public assistance funds awarded to the Plaquemines Parish Sheriff's Office, Louisiana (the Office) to determine whether the Office expended and accounted for FEMA funds according to federal regulations and FEMA guidelines. The Office did not expend and account for FEMA funds, according to federal criteria, nor did it track costs on a project-by-project basis or support cost eligibility. Further, it did not follow federal procurement regulations when it awarded contracts for mobile homes and site preparation. As a result, FEMA has no assurance that costs will be reasonable.

We recommended that the Director, FEMA Louisiana Transitional Recovery Office, in coordination with the grantee and subgrantee: 1) Require the Office to account for each large project separately; 2) Require the Office to provide supporting documentation for disaster costs, 3) Require the Office to comply with federal procurement regulations for all future contracts, and 4) Disallow $1,054,000 for mobile homes purchased but not occupied, and evaluate the remaining costs for eligibility and reasonableness. (DD-07-05, February 2007, DAO)

Contract Costs, Clearbrook , LLC

FEMA awarded a contract to Clearbrook, LLC for base camp services associated with Hurricane Katrina activities in Louisiana. The Office of Disaster Assistance Oversight, Office of Inspector General, conducted an interim review to determine whether FEMA properly administered the contract and whether Clearbrook's billings are reimbursable under the agreements and federal regulations.

The audit determined that as a result of FEMA's haste to establish base camps, and the shortage of trained and experienced contracting officials, the Clearbrook contract was not effectively awarded and administered, leading to contractual deficiencies, excessive billings, and questionable costs of $16.4 million. FEMA's contract administration of Clearbrook's second work order improved significantly and included a reduction in the fixed unit price and a well-defined scope of work.

The audit recommended that the Director, FEMA Louisiana Transitional Recovery Office: 1) Negotiate with Clearbrook to resolve the $32.1 million billed for unoccupied capacity; and 2) Disallow the $16.4 million billed for direct charges and recover any payments already made for these charges. (DD-07-06, February 2007, DAO)

Hurricane Rita Activities – Jefferson County, Texas

We performed an interim review of public assistance funds awarded to Jefferson County, Texas (County). Our objective was to determine whether the County expended and accounted for FEMA funds according to federal regulations and FEMA guidelines. As of

August 25, 2006, the County received an award of $45.6 million from the Texas Governor's Division of Emergency Management, for damages resulting from Hurricane Rita. The award was for 126 FEMA projects. We reviewed costs for four projects totaling $35.1 million, or 77 percent of the award.

In general, the County expended and accounted for FEMA funds according to federal regulations and FEMA guidelines. The County properly accounted for FEMA funds by project and supported project expenditures with invoices, copies of checks, and other documentation. Also, with minor exceptions, the County followed federal procurement regulations to contract for debris removal and monitoring. Therefore, we commend the County and State for a job well done.

Minor issues resulted in questionable costs totaling $239,451. (DD-07-07, March 2007, DAO)

Hurricane Katrina Activities - City of Kenner, Louisiana

We performed an interim review of public assistance funds awarded to the City of Kenner, Louisiana (City). Our objective was to determine whether the City expended and accounted for FEMA funds according to federal regulations and FEMA guidelines. As of August 31, 2006, the City had received an award of $26 million from the Governor's Office of Homeland Security and Emergency Preparedness, for damages resulting from Hurricane Katrina. The award was for 76 FEMA projects. We reviewed the costs for three projects totaling $7 million, or 27 percent of the award.

The City did not track costs on a project-by-project basis or support cost eligibility. If left uncorrected, the City's final claim could include errors and ineligible costs. Further, the City did not follow federal procurement regulations when it awarded $1.4 million in contracts for the purchase of travel trailers. As a result, FEMA has no assurance that costs were reasonable.

We recommended that the Director, FEMA Louisiana Transitional Recovery Office, in coordination with the grantee, (1) require the City to account for each large project separately, (2) require the City to prepare and maintain documentation adequate to support all disaster costs claimed, (3) require the city to comply with federal procurement regulations for all future contracts, (4) evaluate the $1.4 million in contract costs for travel trailers to determine cost reasonableness, (5) provide written guidance to the City for disposition of trailers no longer in use, (6) ensure that applicable insurance proceeds are deducted from approved disaster costs, (7) disallow $679,150 in questionable costs. (DD-07-08, March 2007, DAO)

INVESTIGATIONS

Executive Director of a Private Non-Profit Organization Indicted for Theft of Federal Program Funds, Money Laundering, and Filing False Tax Returns-Update

We initiated an investigation after the Internal Revenue Service, Criminal Investigation Division, reported that the executive director of a private nonprofit organization was suspected in the theft of Federal program funds and submitting false documents to FEMA. Our investigation disclosed that the subject was suspected of submitting over $217,000 in fraudulent claims to FEMA in connection with two disasters. On January 26, 2006, a multicount indictment was returned charging the subject with theft of federal program funds, money laundering, and filing false tax returns. The United States Attorney's Office, Southern District of West Virginia sought the indictment. Subsequent to a trial in United States District Court, the defendant was found guilty on a single count of theft of federal program funds. The defendant was found not guilty on the other counts. On January 5, 2007, the defendant was sentenced to 24 months imprisonment, 36 months supervised release, and ordered to pay $31,129 in restitution and a $10,000 fine.

Four FEMA Employees Arrested and Indicted for Theft

We conducted an investigation into four FEMA employees who devised a scheme to steal air conditioning units from a FEMA storage site in Baton Rouge, LA. On October 4, 2006, the men were arrested after they attempted to sell several of the air conditioning units to an undercover OIG special agent. All four subjects have pleaded guilty to the theft of government property.

Independence, Louisiana Police Department Chief and Captain Plead Guilty

A joint investigation with the Federal Bureau of Investigation (FBI) has resulted in the chief and captain of the Independence Police Department pleading guilty to the theft of government funds. Following Hurricane Katrina, FEMA reimbursed qualifying police departments for overtime hours worked by officers in the aftermath of the storm. By inflating the overtime hours worked by officers within their department, the chief and captain knowingly defrauded the government of more than $1,000. Sentencing is scheduled.

Two men Plead Guilty to Filing Multiple False Claims for FEMA Assistance

We conducted a joint investigation with the United States Postal Inspection Service, Social Security Administration OIG, and the Small Business Administration OIG involving two men who fraudulently obtained $36,000 in disaster assistance benefits by filing applications using 18 different social security numbers and claiming to have suffered damages from Hurricanes Katrina and Rita. The two men were arrested after

being indicted on five counts of wire fraud, 23 counts of mail fraud, and seven counts of identity theft. Both men pleaded guilty to one count of mail fraud and one count of identity theft. One of the men was sentenced to serve 39 months in federal prison, and was ordered to make restitution in the amount of $34, 948. The second man is currently awaiting sentencing.

Five More Charged with Filing Multiple False FEMA Claims –Update

In a joint investigation with the United States Postal Inspection Service, Social Security Administration OIG, and the Small Business Administration OIG, we previously arrested two subjects for falsely filing 39 separate claims that they suffered damages from Hurricanes Katrina and Rita. We subsequently identified five additional subjects who fraudulently obtained over $145,000 in disaster assistance benefits by filing 103 separate applications. Five more individuals were arrested after being indicted for one count of conspiracy, eight counts of mail fraud and three counts of identity theft.

Eleven Indicted for Hurricane Relief Fraud

We conducted a joint investigation with the FBI and the United States Postal Inspection Service that identified 485 suspected fraudulent FEMA applicants residing in Oregon. To date, the investigation has identified 11 suspects in Portland, Oregon, who are responsible for filing 253 fraudulent Hurricane Katrina applications with FEMA, totaling $470,406 in claims. On October 12, 2005, and on January 27, 2006, the 11 suspects were indicted and ten arrested for theft of government property. Eight defendants pleaded guilty to one count of theft of government property and two defendants pleaded guilty to six counts of mail fraud. Nine defendants were sentenced to a total of sixty-three months confinement, twenty-seven years probation, $800 in fines, and $441,184 in restitution. On September 5, 2006, one defendant was sentenced to 21 months confinement, 36 months probation, $100 in fines, and $324,870 in restitution. One suspect remains at large.

Five Indicted for Hurricane Katrina Fraud

We conducted a joint investigation with the FBI, Social Security Administration OIG, and the United States Postal Inspection Service, which identified approximately 36 suspected fraudulent FEMA applications in Fresno and Bakersfield, California. To date, the investigation has identified eight suspects who fraudulently filed Hurricane Katrina applications with FEMA totaling $57,760.26 in claims. Five suspects were indicted for wire fraud, aiding and abetting, filing false claims, mail fraud, and misuse of a social security number. On October 24, 2006, three defendants were sentenced to 36 months probation each with assessments and restitutions. On January 9, 2007, an additional defendant pleaded guilty to wire fraud and aiding and abetting and is scheduled for

sentencing. Additionally, two suspects are pending indictments while a third defendant is pending trial.

Six Indicted for Hurricane Relief Fraud

We conducted a joint investigation with the United States Postal Inspection Service, which identified numerous suspected fraudulent FEMA applications in San Francisco, California. To date, the investigation has identified 22 suspects who fraudulently filed Hurricane Katrina applications with FEMA, totaling approximately $174,742.36 in claims. Six suspects were indicted on charges of theft of government funds. Additional indictments are anticipated.

A Private Citizen Pleaded Guilty to Theft of government Property and Loan Fraud

We conducted a joint investigation with the Social Security Administration OIG, FBI and Department of Education OIG after receiving information that a private citizen knowingly provided false information to FEMA via the Internet in order to receive over $40,000 in Hurricane Katrina relief funds. Our investigation determined that the individual filed three separate applications with FEMA, which contained false information. The individual reported to FEMA that they resided in New Orleans, Louisiana, when Katrina struck, but also reported living in Biloxi, Mississippi, during the same time while actually living in Indianapolis, Indiana. Further investigation determined that the subject also made up false social security numbers to open up accounts at financial institutions and obtained student loans in the amount of $160,000. On January 19, 2007, the private citizen pleaded guilty to the theft of government property, loan fraud, misuse of a social security number and student financial aid fraud and is awaiting sentencing.

Eight Indicted for Hurricane Relief Fraud

We conducted a joint investigation with the FBI, United States Postal Inspection Service, Social Security OIG, Department of Labor OIG, Small Business Administration, and Washington State Department of Social and Health Services, which identified 114 suspected fraudulent FEMA applicants residing in the State of Washington. To date the investigation has identified thirteen suspects who fraudulently filed Hurricane Katrina applications with FEMA, totaling $183,827 in claims. On March 7, 2007, eight suspects were indicted on charges including theft of government property, mail fraud, and false statements. On March 8, 2007, four defendants were arrested and arrest warrants against the remaining four suspects remain outstanding.

Guilty Plea in $100,000 FEMA Hurricane Relief Fund Fraud Scheme

Our investigation, which was conducted jointly with the USSS, Postal Inspection Service, and Department of Treasury OIG, determined that between September and December 2005, an individual applied for emergency FEMA funds in connection with Hurricanes Katrina and Rita, using the names, birth dates, and Social Security numbers of other individuals. As a result of the scheme, FEMA mailed 38 United States Treasury checks, made out to the individuals the subject identified, to the subject's motel or private mailboxes that he rented. The subject then forged the signatures of the payees and deposited the checks into bank accounts that he had opened in the names of other people. On August 28, 2006, the subject pleaded guilty to charges of bank fraud, mail fraud, and money laundering. On February 5, 2007, the defendant was sentenced to 102 months imprisonment, 108 months supervised release, and directed to pay $129,139.81 in restitution.

Forty-Eight Northern Alabama Residents Charged with FEMA Katrina Fraud

A joint investigation with the FBI, USSS, and United States Postal Inspection Service resulted in the indictment and arrest of 48 individuals who claimed to be living in Louisiana at the time Hurricane Katrina struck in August 2005, but actually lived in and around the Birmingham, Alabama, area. The subjects were indicted for filing false claims against the government and were arrested without incident. The false claims resulted in FEMA paying out approximately $300,000. Of the 48 subjects, 26 have entered guilty pleas in Federal court and 22 are pending judicial action.

Multiple Applicants Filed False Claims on Unoccupied Apartment Complex

We conducted an investigation involving 27 individuals who devised a scheme to defraud FEMA by claiming disaster assistance for an apartment complex that was unoccupied at the time of the storm. The apartments were empty and undergoing renovations converting them into condominium units. The subjects were indicted for filing false claims against the government and arrested without incident. The false claims resulted in FEMA paying out in excess of $176,169. No trial dates have been scheduled.

Alabama Residents Filed False FEMA Applications Claiming to Have Lived in Louisiana

We conducted an investigation involving 14 individuals who claimed to be living in Louisiana at the time Hurricane Katrina struck in August 2005, but actually lived in and around the Montgomery, Alabama, area. The primary subjects were a mother and daughter that served as brokers for the other individuals and assisted them in filing their disaster assistance applications. These subjects received a portion of the FEMA funds each individual received as a fee for their services. None of the individuals lived in

Louisiana at the time of the storm. All 14 subjects were indicted for filing false claims against the government and arrested without incident. The false claims resulted in FEMA paying out in excess of $135,000. Eight subjects have entered guilty pleas and are awaiting sentencing. Six subjects are pending trial dates and none have been scheduled as of this date.

Canton, MS, Residents Filed False FEMA Applications Claiming to Have Lived on Mississippi Gulf Coast

We conducted investigations involving several individuals who were living in Canton, Mississippi, and had applied for disaster assistance claiming they lived on the Mississippi Gulf Coast during Hurricane Katrina. Initially we identified twenty-two Canton, Mississippi, individuals, from a loosely related family group, that filed disaster assistance claims using four addresses in Biloxi, Mississippi. We directed a multiagency task force group made up of the FBI, Department of Housing and Urban Development OIG, Department of Labor OIG, United States Department of Agriculture OIG, United States Postal Inspection Service, and the Mississippi State Auditors Office that participated in these investigations. All 22 potential subjects were interviewed the same day by various groups of agents. These interviews revealed that the subjects did not live on the coast as they claimed in their FEMA applications. To date, 12 individuals have been indicted for filing false claims and other criminal violations against the government. The fraud applicable to the 12 indicted subjects is $118,000. No trial dates have been scheduled for the indicted subjects and investigations continue on the remaining individuals.

Two FEMA Employees Pleaded Guilty to Filing False Claim for Disaster Assistance

We conducted an investigation involving two FEMA employees who worked at the Joint Field Office in Biloxi, Mississippi. One subject made a false claim that he owned and lived on a boat at a local marina and the second subject assisted him with false documentation and posing as his landlord to his FEMA inspector. As a result of this claim the subject was awarded $25,562 in disaster assistance. The subjects were indicted by a Grand Jury on multiple counts of defrauding the government. They were arrested at the JFO without incident. Both subjects entered guilty pleas and sentencing is scheduled.

OFFICE FOR CIVIL RIGHTS AND CIVIL LIBERTIES

We received 93 Civil Rights and Civil Liberties complaints from 10/1/2006 to 3/31/2007. Of those, we opened 2 investigations, referred 88 to the Office of Civil Right Civil Liberties with no response requested, and referred 3 with a 30-day response requested. During the reporting period we did not make any arrests, there were no indictments or convictions; and, none of these investigations were resolved.

OFFICE OF INTELLIGENCE AND ANALYSIS

Implementation Challenges Remain In Securing DHS Components' Intelligence Systems

We reviewed Top Secret/Sensitive Compartmented Information systems under DHS' purview. We focused on DHS' information assurance posture, including the policies and procedures in place for the department's intelligence systems. We performed our work at the departmental and organizational component levels, focusing on the system security controls for a subset of intelligence systems, according to the requirements in Director of Central Intelligence Directive 6/3, *Protecting Sensitive Compartmented Information Within Information Systems.*

The objective of our evaluation was to determine whether DHS' information security program and practices are adequate and effective in protecting the information and the systems that support DHS' intelligence operations and assets from unauthorized access, use, disclosure, disruption, modification, or destruction. We also determined whether DHS' privacy program and related activities pertain to its intelligence systems, and whether components have developed or incorporated requirements to protect intelligence system vulnerabilities into their classification guides. Furthermore, we conducted detailed assessments of security controls and documentation for DHS' intelligence systems and assessed the mitigation of system security weaknesses previously identified as a result of system security vulnerability assessments conducted for a subset of intelligence systems in Fiscal Years 2004 and 2005. Fieldwork was conducted from May through August 2006.

DHS formally established the Office of Intelligence and Analysis to implement the department's IT security program for its intelligence systems and assets. We also identified issues regarding the certification and accreditation of DHS' intelligence systems; Plan of Action and Milestones process; incident detection, handling procedures, reporting, and analysis process; and information security training and awareness program for all users of intelligence systems and specialized training for employees with significant security responsibilities for DHS' intelligence systems. We recommended that DHS formally grant the Office of Intelligence and Analysis' Chief Information Officer the comprehensive authority to support the management, operation, and Director of Central Intelligence Directive 6/3 accreditation of the department's intelligence systems, excluding USCG intelligence data systems. DHS management agreed with our recommendation and has begun taking actions to address the issues raised during our review. (OIG-07-15, December 2006, IT)

TRANSPORTATION SECURITY ADMINISTRATION

MANAGEMENT REPORTS

Allegations Regarding San Francisco International Airport

At the request of the TSA, we conducted a review of allegations that TSA officials at San Francisco International Airport had knowingly violated TSA policy and procedures in covering up security breaches at the airport. We also reviewed allegations that TSA and officials of the airport's contract screening company had compromised covert security testing conducted by separate teams from both our office and TSA by broadcasting tester descriptions and methodologies to all screening areas. We conducted our review between May and October 2005.

In general, airport management complied with TSA policy and procedures when identifying and reporting security incidents. However, management should have reported one security incident but did not. Although TSA management could not explain why the incident was not reported, there was no evidence that management acted intentionally to cover up or misreport this or other security incidents.

We confirmed the allegation that TSA and screening company officials at San Francisco International Airport compromised covert security testing, conducted between August 2003 and May 2004, by tracking testers throughout the airport via surveillance cameras and on foot, and then notifying screening personnel in advance of testers arriving at checkpoints. Specifically, descriptions of the testers' physical appearance, clothing, luggage, and test objects were provided to the screening checkpoints by screening company personnel at the direction of a member of TSA management.

We recommended that TSA direct the airport's Federal Security Director to ensure that appropriate members of his staff are trained in and have a thorough knowledge of the guidelines for reporting security incidents to TSA headquarters. Also, we recommended that TSA establish and promulgate policy to regulate its actions in response to authorized covert security testing of checkpoints. (OIG-07-04, October 2006, OA)

Improvements Needed in TSA's Federal Flight Deck Officer Program

We assessed the TSA procedural and process requirements to determine whether they presented barriers to pilot participation and performance in the Federal Flight Deck Officer program. Title XIV of the *Homeland Security Act of 2002*, the *Arming Pilots Against Terrorism Act*, as amended, established the program. This program selects, trains, deputizes, arms with handguns, and supervises volunteer airline pilots and other flight deck crewmembers for the purpose of defending the flight decks of passenger and cargo aircraft.

Our survey identified pilot concerns regarding the program. These concerns included not being given time off to attend training, the remote location of the training and the amount of time used to get to the training site, TSA's weapons carriage policy, and the type of credentials used to identify officers. These concerns may have dissuaded pilots from participating in the program, thus reducing the number of Federal Flight Deck Officers.

In December 2005, management of the program was assigned to TSA's Office of Law Enforcement-Federal Air Marshal Service. This office established focus groups to foster communications among the Federal Flight Deck Officer community, the airline industry, and professional associations, and to address operational concerns. Also, the office management established a program working group to assess recommendations on proposals concerning Federal Flight Deck Officer credentials and badges, checkpoint requirements, weapons issues (including transport, storage, and qualifications), communications protocols, training, and industry liaison.

While TSA has now trained and deputized Federal Flight Deck Officers and has addressed various procedural and process issues, more needs to be accomplished to maximize the use of Federal Flight Deck Officers on international and domestic flights. We recommended that TSA continue to work with the officers, Federal Security Directors, and industry to improve program effectiveness.
(OIG-07-14, December 2006, OA)

Information Technology Matters Related to TSA's FY 2005 Financial Statements

The USCG hosts key financial applications for DHS' TSA. As such, our audit over IT general controls for TSA included a review of USCG's procedures, policies, and practices. While we reported that USGC took corrective actions to address prior year IT control weaknesses that impact the TSA financial processing environment, we continued to find IT general control weaknesses. Collectively, the IT control weaknesses limited TSA's ability to ensure that critical financial and operational data was maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively impacted the internal controls over TSA financial reporting and its operation.

We reported that many of the conditions identified during our prior year audits, which impact TSA financial processing, have not been corrected because challenges continue to exist related to the merging of numerous IT functions, controls, processes, and overall organizational shortages. During FY 2005, USCG took steps to help address known weaknesses, such as conducting periodic vulnerability assessments of security controls, increasing controls over access to sensitive application functions, and implementing practices that adhere to guidance issued in the update to DHS Policy 4300A, *Sensitive System Handbook*.

Despite these improvements, TSA and USCG management should continue emphasis on the monitoring and enforcement of IT security-related policies and procedures. Ongoing measures to certify and accredit key financial systems and implement effective disaster recovery and continuity of operations controls need to be completed. Additionally, many of the repeat vulnerabilities in system access and configuration controls that were determined during technical security testing can be addressed by instituting a formal process for performing scans of USCG's network environment to ensure that security settings, once instituted, remain in place and to determine vulnerabilities that require correction. (OIG-07-18, December 2006, IT)

Access to Airport Secured Areas

Airport operators and aircraft operators each have responsibilities under the Code of Federal Regulations, and their respective approved security programs, to meet certain security requirements. Among these requirements is the responsibility to prevent access by unauthorized persons to defined secured areas of the airport. TSA regulations require personnel who enter the Security Identification Display Area (SIDA) and other secured areas of the airport to have an airport-issued or -approved SIDA badge properly displayed

on their person or to be under escort. No airport operator may grant unescorted access to the secured area or SIDA to any individual unless that person has successfully completed training according to a TSA-approved curriculum specified in the airport security program. The curriculum must include: (1) the unescorted access authority of the individual to enter and be present in various areas of the airport; (2) the control, use, and display of airport-approved access and identification media; and (3) escort and challenge procedures, and the law enforcement support for these procedures.

We conducted more than 600 access control tests at 14 domestic airports of various sizes nationwide. We identified various weaknesses in TSA's procedures, and the implementation of those procedures by airport and air carrier personnel, to prevent unauthorized individuals from gaining access to secured airport areas. We made a total of 10 recommendations that, if implemented by TSA, airport operators, and air carriers, will enhance the overall effectiveness of controls that limit access to airport secured areas. The results of our tests and the recommendations we made to TSA are classified Secret. (OIG-07-35, March 2007, OA)

INVESTIGATIONS

TSA Screener Sentenced for Attempted Sex with a Minor

We initiated an investigation after receiving information that the Riverside County Sheriff's Department arrested a TSA Screener who worked at the Los Angeles International Airport for attempted sex with a minor under the age of 14. The screener pleaded guilty to attempted sex with a minor under 14. On February 23, 2007, he was sentenced to 1 year in jail and 5 years of formal probation and will be required to register as a sex offender pursuant to California Penal Code.

TSA Screener Indicted for Identity Theft

We initiated a joint investigation with the California Department of Motor Vehicles after receipt of an anonymous letter alleging that a TSA Screener was working under an assumed identity. The investigation found that a screener changed the name on a birth certificate and used it to obtain a driver's license and a social security card under an assumed name. She then used the driver's license and the social security card to apply for employment with TSA. The screener is currently being sought on a felony arrest warrant for identity theft.

TSA Security Screener charged with Possession of Methamphetamine

We conducted an investigation into an allegation that a TSA security screener at Seattle/Tacoma International Airport, Seattle, Washington, was involved in possessing methamphetamine on or about October 13, 2006. The screener was terminated by TSA on November 21, 2006. The former screener was arrested on November 24, 2006, for possession of methamphetamine. On February 5, 2007, the former screener was charged with possession of methamphetamine, a state charge.

TSA Security Screener Charged with Possession of Depictions of Minors Engaged in Sexually Explicit Conduct

We conducted an investigation into allegations that a Seattle/Tacoma International Airport, Seattle, Washington, TSA security screener was involved in possessing and dealing in depictions of minors engaged in sexually explicit conduct. The investigation resulted in the arrest of the TSA security screener who was charged with possessing depictions of minors engaged in sexually explicit conduct, a state charge. The TSA security screener was terminated. On October 2, 2006, the TSA security screener pleaded guilty to the state charge and was sentenced to 48 months of "community custody."

TSA Security Screener Charged with Theft

We conducted an investigation into an allegation that a TSA security screener stole $2,000 from a passenger's wallet while screening the passenger at Seattle/Tacoma International Airport, Seattle, Washington. The TSA security screener was arrested and charged with theft. The TSA security screener was terminated. On November 16, 2006, the screener pleaded guilty to theft and was sentenced to 30 days confinement, 12 months probation, and 240 hours of community service.

TSA Security Screeners Charged with Theft

We conducted an investigation into an allegation that three TSA security screeners were stealing prescription medication from passenger carry-on bags at Seattle/Tacoma International Airport, Seattle, Washington. In November 2004, we conducted an undercover operation and subsequently arrested two TSA security screeners. On February 28, 2006, the two TSA security screeners were charged with converting the property of another. On June 21, 2006, both screeners pleaded guilty to the charge in United States District Court. Both screeners resigned in lieu of termination. On October 4, 2006, and October 18, 2006, the two screeners were sentenced to three years probation and two hundred hours of community service.

TSA Security Screeners Charged with Theft

We conducted an investigation into allegations that four TSA security screeners from the Honolulu International Airport were targeting Japanese tourists and stealing Japanese Yen from their checked luggage. In March 2005, one of the TSA security screeners was caught stealing 196,168 in Japanese Yen ($1,800 US) from a passenger's checked luggage. A second TSA security screener was implicated and surrendered 123,000 in Japanese Yen ($1,100 US) that was stolen from checked luggage. Two additional TSA security screeners have been identified. All four TSA security screeners have been terminated. On April 18, 2006, two of the four TSA security screeners pleaded guilty to converting the property of another. On October 16, 2006, two screeners were convicted of the charges and sentenced to 102 days intermittent confinement, 3 years probation, a $2,000 fine, and a $100 special assessment. On February 12, 2007, the United States Attorney's Office declined to prosecute the other two TSA security screeners.

TSA Inspector Arrested for Filing False Inspection Reports

We initiated an investigation after receiving information that a TSA Inspector at the Atlanta Hartsfield Jackson International Airport, Atlanta, GA, submitted eight false reports indicating he performed security inspections at the airport in November and December 2004. The investigation concluded the Inspector did not perform the work and the reports were false. In June 2006, the Inspector was indicted on eight counts of

making false statements. In August 2006, the Inspector entered a guilty plea to the false statement charges. On January 23, 2007, the subject was sentenced to 4 months confinement, 24 months supervised release, and 50 hours of community service.

UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES

MANAGEMENT REPORTS

United States Citizenship and Immigration Services' Progress in Modernizing Information Technology

Effective use of IT, coupled with updated processes, is vital to increase efficiency and address demands in immigration benefits processing. In our September 2005 report, *USCIS Faces Challenges in Modernizing Information Technology* (OIG-05-41), we reported inefficiencies in the United States Citizenship and Immigration Service's (USCIS) operational environment and an unfocused approach to improving processes and systems in order to provide citizenship and immigration services more effectively. In the report, we recommended a number of actions that USCIS can take to leverage IT to achieve its modernization objectives. Such actions also will be critical to support potential increases in benefits processing workloads that could result from proposed immigration reform legislation.

As part of our responsibility for assessing the efficiency and effectiveness of departmental operations, we conducted a review of USCIS' efforts to improve its processes and systems. The objectives of our review were to assess progress in implementing IT modernization initiatives, as well as addressing our prior recommendations.

Although USCIS has taken steps to address the recommendations in our prior report, several challenges continue. Specifically:

- Although USCIS has exhibited new commitment to business transformation, the bureau faces challenges in finalizing its approach and advancing to transformation implementation.
- USCIS has accomplished the first phase of its IT staffing integration effort, however, remaining phases are on hold until the bureau makes necessary organizational improvements to issues that affect day-to-day IT operations.

- USCIS has made progress in applying IT to support mission business operations, but improved strategic planning by the Office of the Chief Information Officer (OCIO) could help in managing IT resources.
- Process engineering is contingent on implementing a "to-be" transaction-based environment and a supporting acquisition approach.
- While significant progress in IT infrastructure upgrades has been made, plans to complete remaining sites are on hold pending funding approval.
- USCIS has outlined strategies to increase stakeholder involvement in transformation planning to promote buy-in and minimize risks that redesigned processes and systems may not meet user needs. (OIG-07-11, November 2006, IT)

INVESTIGATIONS

USCIS Immigration Information Officer Pleads Guilty

We conducted an investigation after receiving information that a package from Nicaragua to the United States was intercepted and contained a foreign passport with an Immigration and Naturalization Service printout. Our investigation identified an Immigration Information Officer complicit in a scheme to assist a Nicaraguan National to obtain legal entry into the United States. The officer denied being involved, but analysis of the passport found the officer's fingerprint on the passport. The officer was arrested and charged with violation of forgery of an official seal, a California state violation. The officer pleaded guilty and was sentenced to 120 days in jail and 3 years probation.

Former CIS Supervisor Accused of Harboring Aliens a Second Time

We conducted an investigation of a former Citizen and Immigration Service (CIS) supervisor, who was previously convicted of harboring aliens and left the government. Subsequently, he was found to be again harboring the same illegal alien after the alien was deported and re-entered the United States illegally. This investigation resulted in a new indictment for the former supervisor and the illegal alien. The former supervisor was arrested on charges of bringing in and harboring aliens. As a result of this investigation, the former supervisor's probation was revoked and he was sentenced to a term of confinement of 8 months and ordered to serve a term of probation of 24 months for violating the conditions of supervision imposed during his previous conviction.

A Private Citizen Arrested for Conspiracy and Immigration Fraud

We opened a joint investigation with ICE Office of Investigations and the FBI after receiving information that a private citizen was acting as an intermediary for an unknown CIS employee who was selling Employment Authorization Documents for $6,000. Our

investigation determined that the private citizen was obtaining legitimate immigration documents for aliens by having them supply fraudulent information. On January 25, 2007, the private citizen was arrested and charged with conspiracy, visa fraud and money laundering and is currently in custody and awaiting trial.

CIS Employee and Co-Conspirator Arrested for Visa, Passport and Identification Fraud-Update

We initiated an investigation after receiving allegations of immigration fraud and bribery by a CIS employee. Subsequent investigation, which was conducted jointly with the FBI, led to the June 29, 2006, arrest of the employee and a co-conspirator for violations of passport fraud, identification fraud, and visa fraud. The arrest warrants were issued by the United States District Court for the Eastern District of Virginia. On October 4, 2006, the fomer employee, who resigned after his arrest, pleaded guilty to one count of bribery and one count of procurement of citizenship or naturalization unlawfully. Sentencing is pending. On October 3, 2006, the co-conspirator pleaded guilty to fraud and misuse of immigration documents; and on December 21, 2006, was sentenced to 21 months imprisonment, 36 months supervised release, and directed to pay a $100 fine.

During the investigation, $4,000 in cash was recovered and forfeited. To date, eight additional subjects, who paid money directly to the employee or through a "broker" to secure the false issuance of U.S. Naturalized Certificates, which were later used to obtain U.S. passports, were indicted in United States District Court for the Eastern District of Virginia for violations of conspiracy and procurement of citizenship or naturalization unlawfully. On January 23, 2007, one subject was found guilty at trial; and on February 26, 2007, two subjects pleaded guilty to one-count of procurement of citizenship or naturalization unlawfully. Arrest warrants have been issued for the remaining five subjects.

UNITED STATES COAST GUARD

Acquisition of the National Security Cutter, U. S. Coast Guard

We assessed the extent to which the USCG's National Security Cutter will meet the cost, schedule, and performance requirements contained in the Integrated Deepwater System ("Deepwater") contract. Deepwater is a $24 billion, 25-year acquisition program to replace and modernize the USCG's aging and deteriorating fleet of ships and aircraft. Deepwater employs a nontraditional "system-of-systems" by which a private sector Systems Integrator is authorized to develop an optimal mix of assets to accomplish all defined USCG Deepwater missions, typically defined as operations more than 50 miles from shore. On June 25, 2002, USCG awarded Integrated Coast Guard Systems a joint

venture between Lockheed Martin and Northrop Grumman, an initial 5-year contract to serve as the Deepwater Systems Integrator. This Deepwater implementation plan specifies that a total of eight National Security Cutters will be built.

As designed and constructed, the National Security Cutter will not meet performance specifications established in the Deepwater contract. Specifically, due to design deficiencies, the structure provides insufficient fatigue strength to meet its contractual performance capability of being underway for 230 days per year, on average, in both the Caribbean (General Atlantic) and Gulf of Alaska (North Pacific) regions over a 30-year operational service life. To mitigate the effects of these deficiencies, USCG intends to task Integrated Coast Guard Systems with modifying the design to support an annual operating profile of 170 to 180 days underway, on average, in the North Pacific region, which is lower than the 230-day performance standard required by contract. The design and performance deficiencies are fundamentally the result of USCG's need to improve technical oversight over the design and construction of its Deepwater assets.

As of November 2006, the combined cost of National Security Cutters 1 and 2 has increased by approximately 50 percent to $775 million from the original $517 million contract estimate. This increase is primarily the result of design changes necessary to meet USCG's expanded post-9/11 mission requirements. However, the current estimate does not include any costs associated with USCG's plan to mitigate the structural deficiencies, additional labor or materials costs resulting from the effects of Hurricane Katrina, or the final cost of a $302 million Request for Equitable Adjustment submitted by Integrated Coast Guard Systems to cover price increases caused by implementation schedule adjustments from June 2002 through January 2005.

Source: U.S. Coast Guard

NSC 1 under construction at NGSS shipyard in Pascagoula, MS.

We made six recommendations, five of which were issued to USCG in order to improve its Deepwater program management oversight and accountability. In order to improve Deepwater contract management oversight and accountability, we also recommended that the Chief Procurement Officer, DHS, in coordination with the department's Office of General Counsel, ensure that all future Deepwater contacts contain terms and conditions clearly stipulating our right of unfettered access to contractor and subcontractor information and personnel. (OIG-07-23, January 2007, OA)

110'/123' Maritime Patrol Boat Modernization Project, United States Coast Guard

In February 2006, our office responded to a Hotline Complaint alleging USCG's eight 123-foot cutters and their short-range prosecutors contained safety and security vulnerabilities. The complaint asserted that the vulnerabilities were incorporated during the conversion of the 110' cutter to the 123' cutter. The complaint also details repeated attempts, over a 2 ½ year period, to compel the contractor to comply with contractual requirements that, if followed, would have alleviated the safety and security vulnerabilities.

Our inquiry into the allegations outlined in the complaint confirmed that aspects of the equipment installed aboard the 123' cutters do not meet the design standards set forth in the Deepwater contract. Specifically, two of the four areas of concern identified by the complainant were substantiated and are the result of the contractor not complying with the design standards identified in the Deepwater contract. For example, the contractor did not install low smoke cabling aboard the 123' cutter as required by the contract. Additionally, the contractor installed equipment aboard both the 123' cutters and prosecutors, which either did not comply or was not tested to ensure compliance with specific environmental performance requirements outlined in the Deepwater contract.

Also, the contractor installed a video surveillance system that failed to provide 360 degrees of coverage. However, the contract did not specify the amount of video coverage the system would provide, therefore the video surveillance system met minimum contract requirements even though video coverage gaps exist.

To address the contract execution and technical oversight concerns and to help prevent similar issues from occurring in the future, we recommended that USCG investigate and address the low smoke cabling and equipment installation issues identified in the Hotline Complaint and take steps to prevent similar technical oversight issues from affecting the remaining surface assets to be modernized or acquired through the Deepwater Program. Additionally we recommended that USCG develop and implement a plan to improve the process for reviewing and adjudicating contractor Requests for Deviations/Waivers. USCG concurred with principle findings of our report and its recommendations, and is in the process of implementing corrective measure. (OIG-07-27, February 2007, OA)

UNITED STATES CUSTOMS AND BORDER PROTECTION

MANAGEMENT REPORTS

Risk Management Advisory for the SBInet Program Initiation

We performed an assessment of risks and controls over DHS' new major acquisition program, Secure Border Initiative network Program (SBInet), which is aimed at transforming border control technology and infrastructure. The SBInet program's objective is to develop solutions to manage, control, and secure the borders using a mix of proven, current, and future technology, infrastructure, personnel, response capability, and processes. SBInet replaces and expands on two previous efforts to gain control of the borders: the Integrated Surveillance Intelligence System and the America's Shield Initiative. The FY 2007 budget request for SBInet included $100 million for border security technology, and similar FY 2008 budget estimates are under development; however, early forecasts and estimates of the program costs range from $8 to $30 billion.

Our objectives were to determine whether lessons learned from other DHS major acquisition programs were being applied to minimize risks to accomplishing SBInet's objectives. By the end of our review, the department was applying lessons learned from previous major acquisition programs. However, the program management office did not have the capability to effectively oversee and assess contractor performance and effectively control cost and schedule. Also, the underlying operational requirements for the program were not properly defined, validated, and stabilized, thereby jeopardizing the program's success and precluding cost and schedule control.

We recommended that the Commissioner, United States Customs and Border Protection (CBP), in coordination with the DHS Chief Procurement Officer, prepare a plan of action and milestones for developing capacity to manage the program, administer its contracts and agreements, and ensure effective oversight and implementation. We also recommended they develop a plan of action and milestones for defining, validating, and stabilizing the program's operational requirements, translating them into contract requirements, and establishing a system of performance metrics and controls to gauge progress in meeting contract requirements and mission needs.
(OIG-07-07, November 2006, OA)

Targeting Oceangoing Cargo Containers

This report is the second annual review of the Automated Targeting System (ATS) used by CBP for sea containers, in response to a congressional mandate in the *Coast Guard and Maritime Transportation Act of 2004*.

CBP did not fully use available information/intelligence sources. Differences in interpreting the Advance Targeting Unit policy exist as to which CBP port personnel need to have security clearances to better affect the targeting mission. In addition, National ATS performance measures are still under development. Also, local controls over container movement and inspection need to be evaluated and improved, and additional guidance for inspection of shipments with elevated ATS scores was needed. Finally, non-intrusive inspection imagery was not always available to CBP Officers conducting cargo inspections.

We recommended that CBP (1) review the use of intelligence from available resources; (2) review security clearances; (3) improve port performance evaluation procedures; (4) refine policies and procedures for identifying and reviewing high-risk shipments; and (5) ensure that non-intrusive inspection imagery is provided to officers conducting secondary level inspections. CBP agreed with our recommendations and outlined planned corrective actions. (OIG-07-09, November 2006, OA)

Improved Administration Can Enhance U.S. Customs and Border Protection Laptop Computer Security

We audited the DHS and its organizational components' security program to determine the security and integrity of select government-issued laptop computers. CBP has employed many essential security controls for its sensitive but unclassified laptops. Our audit work was based on direct observations; vulnerability and wireless system security scans; and an analysis of applicable CBP documents. In addition, we interviewed CBP management officials and security personnel.

Significant work remains for CBP to further strengthen the configuration, patch, and inventory management controls necessary to protect its government-issued laptop computers. Specifically, CBP has not established: (1) a standard configuration for its laptops that meets required minimum-security settings; (2) effective procedures to patch laptop computers; and, (3) adequate inventory management procedures. As a result, sensitive information stored and processed on CBP's laptop computers may not be protected properly. Further, because CBP uses the same procedures to develop a model for its desktop computers, the configuration weaknesses in laptop computers are relevant to all government-issued computers assigned within CBP.

To secure CBP data stored on government-issued laptop computers, we made seven recommendations to the Commissioner of CBP. CBP officials said they have already taken or plan to take corrective action to address the weaknesses.
(OIG-07-16, December 2006, IT))

Independent Auditors' Report on CBP's FY 2006 Consolidated Financial Statements

CBP received an unqualified opinion on its FY 2006 year-end consolidated financial statements, meaning that the consolidated financial statements were presented fairly, in all material respects. The independent public accounting firm KPMG performed the audit.

The auditor reported the following material weaknesses: drawback of duties, taxes, and fees, and information technology. The auditor also reported two additional conditions: (1) financial reporting, specifically in the areas of property, plant, and equipment; intradepartmental imputed financing costs; and financial statement presentation; and (2) entry process, specifically, in the areas of compliance measurement program; bonded warehouse and foreign trade zones; and in-bonded program. Instances of noncompliance with the following laws were also reported: *Federal Information Security Management Act (Electronic Government Act of 2002), Federal Financial Management Improvement Act of 1996 (FFMIA),* and *Improper Payments Information Act of 2002*.
(OIG-07-19, December 2006, OA)

Follow-up on Recommendations from Audit of Procedures to Detect Uranium in Two Smuggling Incidents

In September 2004, we issued an audit report titled, Effectiveness of Customs and Border Protection's Procedures to Detect Uranium in Two Smuggling Incidents. This audit report made four recommendations to enhance the training and search procedures followed by CBP inspectors as well as the effectiveness of the radiation detection equipment. The Chairmen and Ranking Members of four House and Senate Committees requested that we determine the status of CBP's implementation of the recommendations.

CBP is making progress in implementing the recommendations by continuing to improve its container examination process and radiation portal monitor operations. Specifically, it has revised its container inspection training; installed software enhancements in Radiation Portal Monitors; is working with the Domestic Nuclear Detection Office and DHS' Science and Technology Directorate officials and the Department of Energy scientists to improve the detection capability of radiation portal monitors by evaluating the next generation of these monitors.

CBP's improvements to the container inspection process and radiation detection equipment capabilities should continue to improve, as its officers become more experienced and new technologies are incorporated into detection equipment.
(OIG-07-30, February 2007, OA)

Customs and Border Protection's Agriculture Inspection Activities

We conducted a joint review with the United States Department of Agriculture (USDA) OIG of selected agricultural inspection activities that were transferred to CBP from USDA. With the DHS creation in March 2003, CBP assumed responsibility to inspect agricultural goods arriving at U.S. ports while USDA-Animal and Plant Health Inspection Service retained responsibility for agriculture related policies and procedures.

CBP generally conducted agriculture inspection activities in compliance with procedures at ports visited. However, improvements were needed to ensure that Agricultural Quarantine Inspection Monitoring sampling, staffing, and performance measures are adequate. CBP's agricultural quarantine sampling, which helps USDA predict potential future risks to agriculture from pests and diseases, did not meet sampling requirements for 13 of 18 pathway activities at four ports (such as air passengers and truck cargo agricultural inspections). CBP also needed a current staffing model for agriculture specialists and performance measures for many activities to ensure the most effective use of personnel.

We identified other noncompliance and control issues. At Miami CBP agriculture specialists were not following proper procedures for selecting flower samples for inspection. Miami CBP also made an operational change to procedures for inspections of cut flowers but did not have a specific formal process for notifying USDA concerning this change. This affects the inspection practices for 87 percent of the cut flowers entering the United States. In addition, CBP ports did not adequately monitor Transportation and Exportation shipments. We also reported significant inaccuracies in data used to track agriculture inspection activities. For example, 107 of 148 Work Accomplishment Data System activity codes were reported incorrectly or did not have supporting documentation to allow verification.

We made ten recommendations to CBP and USDA-OIG made three recommendations to USDA-Animal and Plant Health Inspection Services that address the deficiencies we identified. CBP and USDA concurred with our recommendations and took appropriate corrective actions. (OIG-07-32, February 2007, OA)

INVESTIGATIONS

Border Patrol Agent indicted for civil rights violation, tampering with a victim and making false statements

Our investigation, conducted jointly with the FBI, determined that a Senior Border Patrol Agent kidnapped and made sexual contact with two aliens, a mother and her minor

daughter in March 2004. The agent had detained the mother and her daughter for crossing the Mexico border and entering into the United States illegally. The agent allowed the mother and the daughter to return to Mexico without processing their illegal entry into the United States. The agent is under indictment and is awaiting trial. When questioned, the Senior Border Patrol Agent lied and claimed that he had not engaged in sexual contact with the females and claimed that he had not detained the undocumented aliens.

CBP Officer Arrested for Alien Smuggling

We initiated an investigation after receiving information that a DHS employee was assisting a smuggling organization. Working with the Border Corruption Task Force, we discovered that the employee had received thousands of dollars from the smugglers. The employee was arrested along with the two smugglers. One smuggler pleaded guilty to alien smuggling and was sentenced to 41 months confinement. During February 2007, the employee pleaded guilty to alien smuggling and bribery. He was sentenced to 60 months confinement, 36 months probation, and fined $200,000.

Border Patrol Agent Arrested for Alien Smuggling

We initiated an investigation after receiving information that a Border Patrol Agent was assisting an alien smuggling organization. Surveillance disclosed that during his off duty hours, he provided escort for the smugglers' vehicles as they traveled into Southern California. During June 2006, one of the smuggling organization's drivers was arrested for narcotics possession. When arrested, the driver was transporting four illegal aliens. The driver provided information on the organization's activities. During January 2007, the agent was arrested along with four co-conspirators. They were charged with violations of alien smuggling.

Border Patrol Agent Arrested for Attempted Lewd Act Upon a Child

On January 26, 2006, we received information that a 14-year-old girl was receiving e-mails of a sexual nature from an El Centro Border Patrol Agent. The investigation was conducted jointly with the California Department of Justice and ICE-Office of Investigations. On January 29, 2007, an undercover e-mail conversation was conducted with the agent and an undercover call was placed to the agent. The agent agreed to meet with the child and was subsequently arrested at the prearranged meeting location. On January 31, 2007, the agent was charged with attempted lewd act upon a child.

Two CBP Officers Accused of Harboring Illegal Aliens

We conducted an investigation of two CBP Officers engaged in harboring and transporting illegal aliens. One officer engaged in a personal relationship with an alien

while the other aided and abetted the officer by attempting to obtain immigration benefits for the alien. The investigation resulted in indictments and arrests of both CBP officers on charges of bringing in and harboring aliens. Both aliens were arrested for entry without inspection and deported.

Border Patrol Agent Investigated for Human Smuggling through Airport

We conducted an investigation concerning allegations that a Border Patrol Agent was involved in Human Smuggling activity through the Miller International Airport, McAllen, Texas. The investigation disclosed the existence of an organized alien smuggling ring using the airport, and resulted in the arrests of several undocumented aliens. The criminal investigation was concluded when the Border Patrol Agent was terminated from his employment with the CBP for numerous administrative violations.

CBP Officer Arrested In National Sweep for Child Pornography

We participated with ICE in the joint execution of a search warrant on the residence of a CBP officer in New Jersey. That search produced evidence that the officer had purchased child pornography via the Internet. The officer was subsequently arrested and prosecution is ongoing in the District of New Jersey.

A Canadian Citizen Arrested for Smuggling Marijuana

On January 29, 2007, as a result of information we developed during a joint investigation with ICE-Office of Investigations into an allegation of a smuggling scheme involving a corrupt CBP Officer, a Canadian citizen was arrested after he attempted to enter the United States driving a truck carrying 55 pounds of marijuana. The investigation did not implicate any CBP Officer in wrongdoing.

CBP Officer charged with Importation of a Controlled Substance

We conducted an investigation into an allegation that a Blaine, Washington, Port of Entry CBP officer was involved with importing marijuana. The investigation revealed that the officer had accepted currency and sexual favors in return for being influenced in the performance of his official duties, and failed to prevent the introduction of contraband into the United States, and aided and abetted in the importation of one hundred or more kilograms of marijuana. On October 24, 2006, the officer was indicted for importation of a controlled substance and bribery of a public official. On November 22, 2006, the CBP officer was terminated.

A Detroit Resident Indicted for Impersonation of a Federal Agent

We conducted an investigation of a private citizen who claimed to be a federal agent working for DHS. The private citizen stated that he had access to law enforcement reports and other case sensitive information, including FBI investigative reports, which he was willing to sell. We initiated an undercover investigation in the course of which the private citizen accepted $600 and promised to provide a comprehensive report of an FBI criminal investigation. On May 5, 2006, the private citizen was indicted in the Eastern District of Michigan for impersonation of a federal agent. An arrest warrant is still outstanding.

Sale of Fraudulent Immigration Documents

We conducted an investigation of a fraudulent immigration document vendor, who was accused of conspiring with an unidentified CBP Officer to provide legitimate immigration documents to unqualified persons who sought to enter the United States unlawfully. We used government "buy-money" to obtain from the subject Arrival/Departure Records, Forms I-94, for fictitious individuals. On September 27, 2006, a Federal Grand Jury indicted the subject on two counts of the transfer and sale of counterfeit identification documents and two counts of visa fraud. On October 5, 2006, the subject was arrested as he attempted to enter the United States through the San Luis Port of Entry, San Luis, Arizona. A custodial interview of the subject revealed no CBP employee involvement in the fraudulent document scheme. On February 5, 2007, the subject pleaded guilty to the charges listed above. Sentencing is scheduled.

Border Patrol Agent Charged with Theft of Public Property and Money

We conducted an investigation into a CBP Border Patrol Agent assigned to the Tucson Sector for theft of public property and money. The investigation disclosed that the subject had purchased more than 30 motorcycle tires and 10 motorcycle inner tubes with government funds, then sold them to an auto-parts store for $2,750 and kept the money. Additionally, the subject charged $1,000 to a government fleet card to pay for enhancements to a golf cart that was to be given to another individual. On December 20, 2006, a Federal Grand Jury indicted the subject for two counts of theft of public property and money.

CBP Officer Convicted of Child Abuse and Molestation

We conducted a joint investigation with the FBI and ICE, Office of Professional Responsibility, into an allegation of narcotics trafficking by a CBP Officer. On July 20, 2004, the subject was arrested after taking possession of two kilograms of cocaine during a controlled delivery. We obtained a federal search warrant for the subject's residence.

During the execution of the search warrant video evidence was discovered showing the subject molesting his minor child. On February 28, 2007, after a jury trial in state court, the jury convicted the subject on 317 counts of molestation of a child, sexual conduct with a minor, sexual exploitation of a minor and child abuse. The subject can be sentenced to 12,000 years in prison. The subject is also pending federal narcotic and child pornography charges. Three civilians have pleaded guilty to narcotics conspiracy charges.

Former Border Patrol Lead Intelligence Agent is sentenced to 3 years of supervised probation following guilty plea

As a result of our investigation, a United States Border Patrol Lead Intelligence Agent pleaded guilty to stealing an ATM visa check card from another United States Border Patrol Agent. The employee committed forgery while making numerous fraudulent purchases with the ATM card. Prior to pleading guilty, the employee's bond was revoked and was placed back into custody after testing positive for cocaine. On November 27, 2006, the employee was sentenced to 3 years supervised probation and ordered to participate in a mental health treatment program and in a drug/alcohol treatment program.

UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT

MANAGEMENT REPORTS

Treatment of Immigration Detainees Housed at Immigration and Customs Enforcement Facilities

We assessed the extent to which ICE facilities that house immigration detainees were complying with detention standards. We focused on detention standards regarding Health Care, Environmental Health and Safety, General Conditions of Confinement, and Reporting of Abuse at five facilities used by ICE. The five facilities were:

- Berks County Prison, Leesport, Pennsylvania;
- Corrections Corporation of America Facility, San Diego, California;
- Hudson County Correction Center, Kearny, New Jersey;
- Krome Service Processing Center, Miami, Florida; and
- Passaic County Jail, Paterson, New Jersey.

All five facilities had instances of noncompliance with ICE Detention Standards. Regarding health care standards, four of the five detention facilities had instances of noncompliance, including timely initial and responsive medical care. Three of the five detention facilities reviewed had environmental health and safety concerns. Instances of noncompliance with ICE Detention Standards regarding general conditions of confinement at the five facilities included: disciplinary policy, classifying detainees, and housing together detainees classified at different security levels. Two facilities also had inadequate inventory controls over detainee funds and personal property. Further, the ICE Detention Standard on Detainee Grievance Procedures does not provide a process for detainees to report abuse or civil rights violations. In addition, two detention facilities did not issue handbooks specifically addressing detainee's rights, responsibilities, and rules, and three facilities did not translate handbooks and orientation material into Spanish and other prevalent languages.

When we brought these concerns to the attention of ICE management, ICE took immediate action. We made 12 recommendations that address each of the areas needing improvement to ensure that the quality of the environment for detainees in ICE's care is adequate to protect their health, safety, security, and well being.
(OIG-07-01, December 2006, OA)

United States Immigration and Customs Enforcement's Detainee Tracking Process

We assessed the ICE detainee tracking process to determine whether ICE had an effective system to track the location of detainees and respond to public inquiries. ICE is responsible for immigration investigations and detention and removal of illegal aliens. The detainee tracking system, for five of the eight ICE detention facilities tested, did not always contain timely information. At the five facilities, data for 10 percent of the detainees examined were not recorded in the Deportable Alien Control System (DACS) within the first 5 days of detainment. ICE procedures were to record detainee data in DACS as soon as possible, usually within 2business days from the date of detainment.

At six of eight ICE detention facilities tested, DACS and detention facility records did not always agree on the location of detainees, or contained information showing the detainee had been deported. At one detention facility, ICE overpaid the facility $9,620 for eight detainees who had been released. At the same time, ICE underpaid the detention facility $1,665 for two detainees who were being held, but not identified in DACS. ICE had no formal policy regarding what information it would provide to anyone inquiring about detainees in their custody. However, the four field offices we visited and the eight detention facilities contacted said that they would confirm whether the detainee was held in their facility. Requests for more detailed information would be referred to ICE headquarters.

We made three recommendations, with which ICE concurred and took appropriate corrective actions. ICE will issue guidance to the field addressing timely DACS entries, supervisory reviews, and periodic reconciliation of DACS data. ICE will also work with the appropriate officials to recover the overpayments. (OIG-07-08, November 2006, OA)

ICE's Compliance With Detention Limits for Aliens With a Final Order of Removal From the United States

ICE Office of Detention and Removal Operations manages the detention and deportation of aliens with a final order of removal from the United States. In addition to current laws, regulations, and internal guidance, this office must comply with two Supreme Court rulings that generally prohibit periods of detention longer than 6 months for some aliens, unless certain conditions apply. We reviewed ICE's compliance with detention time limits for aliens with a final order of removal, including the reasons for exceptions or noncompliance. We focused on: (1) compliance with the Supreme Court rulings in Zadvydas v. Davis 533 U.S. 678 (2001) and Clark v. Martinez 543 U.S. 371 (2005), and implementing regulations; (2) the quality of guidance provided by DRO headquarters; and (3) ICE's management practices, including its ability to track and prioritize cases and conduct nationwide quality assurance.

ICE has introduced quality assurance and tracking measures for case review; however, outdated databases and current staffing resources limit the effectiveness of its oversight capabilities. Although approximately 80 percent of aliens with a final order are removed or released within 90 days of an order, ICE's Post-Order Custody Reviews for the remaining cases were not conducted in more than 6 percent of cases, and were not performed on time in more than 19 percent of cases. Moreover, some aliens have been suspended from the review process without properly documented evidence that the alien is failing to comply with efforts to secure removal. In addition, cases are not prioritized to ensure that aliens who are dangerous or whose departure is in the national interest are removed, or that their release within the United States is properly supervised. Finally, ICE has not provided sufficient guidance on applying the Supreme Court's "reasonably foreseeable future" standard, and does not systematically track removal rates—information that is necessary for negotiating returns and for determining whether detention space is used effectively.

Our report contains five recommendations: (1) holding ICE field offices more accountable for the quality and timeliness of the POCR process; (2) increasing ICE headquarters assistance in obtaining travel documents; (3) prioritizing the removal of aliens who represent a serious threat to society or the public interest; (4) developing an objective and transparent methodology for evaluating the likelihood of removal for all cases; and (5) intensifying the monitoring of long-term detainees.
(OIG-07-28, February 2007, ISP)

An Assessment of United States Immigration and Customs Enforcement's Fugitive Operations Teams

We assessed ICE's Fugitive Operations Teams. The purpose of our review was to determine the adequacy of the performance measures used to assess the Fugitive Operations Teams and to review the teams' progress in reducing the backlog of fugitive alien cases. We assessed the adequacy of the teams' staffing levels resulting from additional funding and the Office of Detention and Removal Operations' recruitment efforts. Lastly, we reviewed factors affecting the teams' operations, such as coordination activities with internal and external entities and the Office of Detention and Removal Operations' training policies.

The fugitive alien apprehensions reported by ICE's Office of Detention and Removal Operations did not accurately reflect the teams' activities and the fugitive alien backlog increased despite the teams' efforts. The teams' effectiveness was limited by insufficient detention space, the functionality of an immigration database, and inadequate working space. We could not determine the removal rate of fugitives apprehended by the teams and the teams performed duties unrelated to fugitive operations, contrary to Office of Detention and Removal Operations policy. Despite hiring obstacles, progress has been made in staffing the teams. The teams also have effective partnerships with federal, state, and local agencies and have basic law enforcement training.

We made seven recommendations to the Assistant Secretary for United States Immigration and Customs Enforcement to address our concerns. The Office of Detention and Removal Operations has taken steps to improve its operations. The office has: (1) developed a reporting system to track enforcement activities based on various categories of apprehensions; (2) established information-sharing agreements with federal, state and local entities to obtain data on fugitive aliens and continues to pursue others; (3) provided additional administrative support to the teams through the creation of the Fugitive Operations Support Center; (4) increased the efficiency of existing detention and removal resources through improved management and coordination of the movement and placement of detained aliens; and (5) acquired 6,300 additional bed spaces since November 2005. (OIG-07-34, March 2007, ISP)

Federal Protective Service Needs To Improve Its Oversight of the Contract Guard Program

We assessed the Federal Protective Service's (FPS) contract guard monitoring efforts within its National Capital Region (Region 11) to determine whether effective controls are in place to ensure qualified contract guards are deployed at federal buildings and if FPS effectively monitors contractor performance and compliance with contract provisions. In addition, we assessed the extent to which contract guard company invoices were paid on time according to the Prompt Payment Act.

We concluded that FPS' Region 11 is not consistently deploying qualified and certified contract guards because FPS personnel were not effectively monitoring the contract guard program. Contract guards were on post without current suitability determinations or with expired certifications. Also, security contractors were not performing their security services according to the terms and conditions of their contracts. In addition, FPS is not paying invoices in a timely manner for its contract guard services nationwide and is in violation of the Prompt Payment Act. Of the 25,557 invoices paid from October 1, 2004, to November 21, 2005, only 12 percent were paid within 30 days, as required by the Prompt Payment Act. This condition occurred, in part, because the FPS transition from the General Services Administration's Financial Management System to the ICE Federal Financial Management System was improperly planned. As a result, FPS paid more than $1.2 million in interest to guard companies that are contracted by FPS to protect federal buildings for late payments made during this time period.

We recommended that the Regional Director of the National Capital Region: (1) ensure that NCR Area Commanders properly monitor Quality Assurance Specialists' inspection reports for quality and timeliness, and provide training for specialists found to be in need of improvement; (2) provide the necessary resources to the Contract Section to ensure the timely processing of proposed deduction letters; (3) establish effective systems and procedures to track the status of inspection reports and proposed deduction letters to ensure guard company compliance with contract requirements; (4) review all inspection reports and proposed deductions for the period March 1, 2003, through the present and initiate collection actions on all contracts found to be deficient; and (5) work with ICE's Chief Financial Officer to implement corrective actions to properly address improvements needed in internal control and payment timeliness issues reported here and in our annual financial audit report issued in November 2005.
(OIG-07-05, October 2006)

INVESTIGATIONS

Federal Protective Service Officer Pleads Guilty to Conspiracy

We conducted an investigation into allegations that a former FPS Physical Security Specialist and Contracting Officer Representative accepted plane tickets and trips to participate in golf tournaments from a DHS security contractor, in exchange for references for future contracts. The former officer pleaded guilty to one count of conspiracy, bribery, and false statements.

Federal Protective Service Inspector Convicted of Embezzlement of Union Funds

We received information from The Fraternal Order of Police, FPS Labor Committee, of financial irregularities with management of union funds in the New York Branch of the

Fraternal Order of Police. Our investigation determined that between June 19, 2003, and January 26, 2005, the Treasurer, an FPS Inspector assigned in New York City, had stolen $23,326.94 in union funds by writing and negotiating checks payable to "cash" and withdrawals through automated teller machines. The inspector was convicted in the Southern District of New York, placed on 3 years probation with the condition of full restitution, and subsequently resigned from the FPS.

Immigration Enforcement Agent Exonerated for Bribery

We received similar allegations from United States Attorneys in both Massachusetts and New Hampshire that a Boston Immigration Enforcement Agent was extorting bribes from aliens, fabricating evidence, and cooperating with a prostitution ring in the control and discipline of alien employees with threats of deportation. We determined the alien source of the allegations could provide no corroboration for, or evidence of, the extortion or the fabrication of evidence. We did determine that the allegations against the agent were made in retaliation for his aggressive enforcement action. Our investigation also determined that a Brazilian alien prostitute, who had previously provided information regarding illegal alien activity to the agent, used false claims of influence with the agent to threaten alien employees with deportation as a method of control in her organization.

One Indicted for Theft and Embezzlement of government Funds

We conducted an investigation into an allegation that an ICE timekeeper embezzled approximately $37,000 of government funds by devising a scheme to add fraudulent overtime hours, as well as annual/sick leave hours, to her own payroll records. The suspect subsequently resigned from ICE. On August 31, 2006, the suspect was indicted for the theft/embezzlement of public money. The defendant pleaded guilty and is awaiting sentencing.

Immigration Enforcement Agent resigned after being charged with Providing False Statements

We opened an investigation after receiving information from a private immigration attorney who alleged that an Immigration Enforcement Agent was accepting money from aliens in exchange for arranging their release from ICE custody by placing them into the Electronic Monitoring Device Program. Our investigation determined that the agent released an Iraqi citizen from ICE custody in exchange for employment consideration for the agent's spouse. We interviewed the agent who admitted to providing false information to us while under oath. The subject was arrested and charged with making false statements and bribery and is awaiting sentencing. On January 25, 2007, the agent resigned from duty.

Supervisory Immigration Enforcement Agent indicted on four counts of Fraud and False Statements

On March 7, 2007, our investigation led to the indictment of a Supervisory Immigration Enforcement Agent on four counts of fraud and false statements. A bench warrant was requested for his arrest and is pending. The employee provided false statements in an application to the Department for Housing and Urban Development for the purpose of securing a loan through the "Officer Next Door" program. In doing so, the agent unlawfully profited by renting out the property. At the time of the crime, the employee was serving as an agent with the United States Border Patrol.

MULTICOMPONENTS

MANAGEMEMT REPORT

Technical Security Activities at Dulles International Airport

We evaluated the DHS and its organizational components' security programs at Dulles International Airport. Our objective was to determine whether the DHS components at the airport complied with the department's technical and information security policies and procedures. Specifically, we assessed how CBP and the TSA had implemented computer security operational, technical, and managerial controls for their information technology assets at this site.

This evaluation included onsite verification and validation of operational security controls, evaluation of technical security controls implemented on their servers, and reviews of applicable DHS policies, procedures, and other appropriate documentation. We briefed the DHS Chief Information Security Officer and the DHS components on the results of our evaluation. We also made nine recommendations to improve information technology security at the airport. DHS concurred with our recommendations and directed the components to address the findings. (OIG-07-25, January 2007, IT)

Major Management Challenges Facing the Department of Homeland

We assessed the management challenges facing the DHS, as required annually by the *Reports Consolidation Act of 2000*. These challenges were included in DHS' *Fiscal Year 2006 Performance and Accountability Report*. We identified the following as the major management challenges facing DHS in Fiscal Year 2007.

Catastrophic Disaster Response and Recovery
Acquisition and Contract Management

Grants Management
Financial Management
Information Technology Management
Infrastructure Protection
Border Security
Transportation Security
Trade Operations and Security

Since its inception in 2003, DHS has worked to accomplish the largest reorganization of the federal government in more than half a century. This task, creating the third largest Cabinet agency with the missions of protecting the country against another terrorist attack, responding to threats and hazards, ensuring safe and secure borders, welcoming lawful immigrants and visitors, and promoting the free flow of commerce, has presented many challenges to its managers and employees. While DHS has made progress, it still has much to do to establish a cohesive, efficient, and effective organization. We have made recommendations in many, but not all, of these areas as a result of our reviews and audits of departmental operations. (OIG-07-12, December 2006, OA)

OTHER OIG ACTIVITIES

FPS TRAINING ACADEMY RECOGNIZES INDIVIDUAL CONTRIBUTIONS

On February 7, 2007, a breakfast was held at the FPS Training Academy to recognize a number of individuals for their contributions in the case of the *United States of America v. Robert T. Schofield, et al*.

Principal Deputy Inspector General Jim Taylor presented DHS OIG Certificates of appreciation to Deputy District Director Susan Dibbins, USCIS; SA James Izzard, Jr., DHS OIG; SA Nadim Abdush-Shahid, DSS; Anti-Fraud Officer Herman Buckley, USCIS; AUSA Ronald Walutes, EDVA; SA Pamela Bombardi, FBI; SSA Dean McDonald, ICE; SA Jennifer Bach, FBI; and Second Lieutenant Gun S. Lee, FCPD

Oversight of Non-DHS OIG Audits

We processed 49 contract audits conducted by DCAA during the current reporting period. Of the DCAA reports processed, one report contained $353,701 in questioned costs, of which all were unsupported, and two reports contained $469,074 in funds put to better use. We continue to monitor the actions taken to implement the recommendations in the reports.

We also processed 57 single audit reports issued by other independent public accountant organizations. The single audit reports questioned $13,607,327, of which $3,607,816 was determined to be unsupported. The reports were conducted according to the *Single Audit Act of 1996,* as amended by PL 104-136. We continue to monitor the actions taken to implement the recommendations in the reports.

Significant Reports Unresolved Over 6 Months

Timely resolution of outstanding audit recommendations continues to be a priority of both our office and the department. As of this report date, we are responsible for monitoring 199 reports that contain recommendations that have been unresolved for more than 6 months. Management decisions have not been made for significant reports, as follows:

- **69 program management reports**

  The department is currently reviewing the reports and advises that it anticipates resolving the recommendations by September 30, 2007.

- **65 grant compliance reports**

  The department is currently reviewing the reports and advises that it anticipates resolving the recommendations by September 30, 2007.

- **19 state disaster management contract audit reports**

  The department is currently reviewing the reports and advises that it anticipates resolving the recommendations by September 30, 2007.

- **7 inspection reports**

  The department is currently reviewing the reports and advises that it anticipates resolving the recommendations by September 30, 2007.

- **12 Single Audit Act reports**

  The department is currently reviewing the reports and advises that it anticipates resolving the recommendations by September 30, 2007.

- **22 Defense Contract Audit Agency reports**

  The department is currently reviewing the reports and advises that it anticipates resolving the recommendations by September 30, 2007.

- **5 legacy agency audit reports**

  The department is currently reviewing the reports and advises that it anticipates resolving the recommendations by September 30, 2007.

LEGISLATIVE AND REGULATORY REVIEW

Section 4 (a) of *the Inspector General Act of 1978*, as amended, requires the Inspector General to review existing and proposed legislation and regulations relating to DHS programs and operations and to make recommendations concerning their potential impact. Our comments and recommendations focus on the impact of the proposed legislation and regulations on economy and efficiency in administering DHS programs and operations or on the prevention and detection of fraud and abuse in DHS programs and operations. We also participate on the President's Council on Integrity and Efficiency, which provides a mechanism to comment on existing and proposed legislation and regulations that have a government-wide impact.

During this reporting period, we reviewed 58 legislative and regulatory proposals, draft DHS policy directives, and other items. Some of these items are highlighted below.

OIG Access Issues. We responded to congressional questions for the record regarding our access to DHS employees, contractors, and documents during audits. We expressed our interest in working with Congress to provide clarification, possibly through legislation or clarifying report language, to ensure our office has unfettered access to personnel and documents, as provided in the Inspector General Act.

Homeland Security Acquisition Regulation (HSAR). We reviewed the department's proposal to amend the HSAR to reflect a statutory change restricting the length of certain noncompetitive contracts DHS enters into in response to or recovery from natural disasters, terrorist acts, or other man-made disasters. We noted that the proposed regulation would have narrowed the statute's applicability to contracts for presidentially declared disasters and events of national significance. Therefore, we recommended changes to ensure the statute will be fully implemented. The department agreed with our recommended changes.

Homeland Security Information Network (HSIN). We reviewed two planning documents establishing HSIN's strategic framework and implementation plan. We provided several comments regarding the discussion and involvement of state, local, tribal, and private industry stakeholders. Overall, the strategic framework and implementation plan seemed to focus primarily on DHS components, without mentioning external stakeholders. As such, the implementation plan did not address how all stakeholders, not just DHS components, would be involved in the system development lifecycle process. In addition, the strategic framework referred to mapping HSIN's capabilities to the mission goals, priorities, and activities of the department. However, there was no mention of how this information would be communicated to all system users, including those in the state, local, tribal, and private industry communities. We

also noted that the planning documents did not indicate how HSIN relates to or will integrate with other related systems.

National Response Plan (NRP) and National Incident Management System (NIMS). We reviewed draft revisions to the NRP and NIMS. We suggested that categories used in the resource typing protocol for the NIMS correspond with the emergency support functions outlined in the NRP. This would better describe the relationship between the NIMS and NRP, as well as better aid resource decision-making during an incident.

Disaster Recovery Survey of Business. DHS proposed using a written survey to collect information from businesses regarding the economic impacts following disasters. We expressed concern about the limited use of the survey results and the survey's promise of confidentiality. Therefore, we suggested changes to ensure the information collected could also be used for civil and criminal enforcement.

CONGRESSIONAL BRIEFINGS AND TESTIMONY

Our office met with members of Congress and their committee staff on numerous occasions to discuss results of our work including our review of the USCG National Security Cutter and the Deepwater's 123-foot maritime patrol boat program, SBInet, Federal Protective Service funds transferred from the General Services Administration to DHS, the TSA's continuity of operations plan programs, financial management at the department, and our fiscal year 2008 budget.

Additionally, we met with congressional members and staff to discuss legislatively mandated and congressionally requested reviews including the World Trade Center Captive Insurance Company, the ADVISE program, allegations of mismanagement at Jackson-Evers International Airport, a review of TSA's national screening force, the department's contracts with Shirlington Limousine and Transportation company, and evaluating the management of DHS operations overseas.

Our office testified before the congress eight times during this reporting period on a wide range of topics including ICE detention and removal activities, department procurement practices including Deepwater and SBInet, and major challenges facing FEMA and the department. We presented testimony at the following congressional hearings:

- March 27, 2007 – Subcommittee on Homeland Security, Committee on Appropriations, United States House of Representatives, entitled, "Priorities in Enforcing Immigration Laws and Temporary Worker Programs."

- March 14, 2007 – Subcommittee on Homeland Security, Committee on Appropriations, United States House of Representatives, to discuss the major management challenges facing the reform of FEMA.

- February 28, 2007 – Subcommittee on Emergency Communications, Preparedness, and Response, and Subcommittee on Management, Investigations, and Oversight, Committee on Homeland Security, United States House of Representatives, on the major management challenges facing the reform of FEMA.

- February 14, 2007 – Subcommittee on Oceans, Atmosphere, Fisheries and USCG, Committee on Commerce, Science and Transportation, United States Senate to discuss the status of USCG's Deepwater Program.

- February 8, 2007 – Committee on Oversight and Government Reform, United States House of Representatives, on the procurement practices of DHS.

- February 7, 2007 – Committee on Homeland Security, United States House of Representatives, entitled, "An Overview of Issues and Challenges Facing the Department of Homeland Security."

- February 6, 2007 – Subcommittee on Homeland Security, Committee on Appropriations, United States House of Representatives, to discuss major management challenges facing DHS.

- November 15, 2007 – Subcommittee on Management, Integration, and Oversight, Committee on Homeland Security, United States House of Representatives, to discuss our risk management review of the SBInet program initiative.

Testimonies for these hearings are available on our website: www.dhs.gov/oig, under the heading "Reports and Resources," subheading, "Congressional Testimonies."

SCORECARD FOR SELECTED ACQUISITION FUNCTIONS AT THE DEPARTMENT OF HOMELAND SECURITY

OVERVIEW

We are publishing the first of what will be a series of scorecards identifying the progress made in selected acquisition functions and activities within the DHS. The purpose of these scorecards is to summarize previously issued audits and inspections, supplemented by additional fieldwork. This section includes scorecards for the acquisition operations in DHS as a whole and at the FEMA. We also assessed the individual acquisition activities for the Coast Guard's Integrated Deepwater System Program (Deepwater) and CBP' Secure Border Initiative network Program (SBInet).

The data included in the scorecards reflect our audits and inspections reports issued through March 2007, as well as additional fieldwork conducted in February and March 2007. Our focus was on specific areas within acquisition management. The nature and brevity of this review precluded our normal audit protocol; therefore, this review was not conducted according to generally accepted government auditing standards. Had we followed such standards, other matters may have come to our attention.

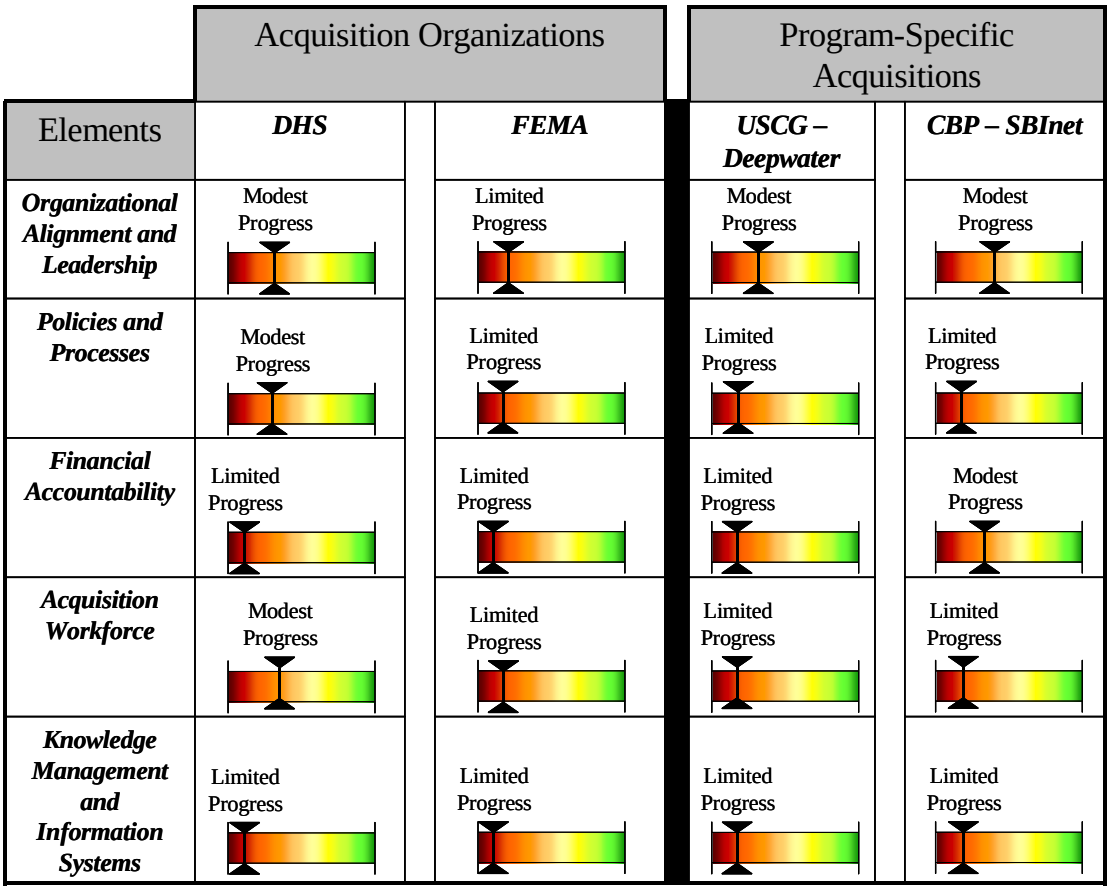
To achieve our purpose, fieldwork included interviews with DHS acquisition officials; reviews of relevant reports and testimony (FY 2003 to present) from our office, the Government Accountability Office (GAO), and DHS management; reviews of policies, directives, procedures, and guidelines relating to DHS acquisition and management; reviews of supporting data requested from DHS and comparison of this data to information collected from interviews and other sources; and analysis of acquisition, budget, and workforce data obtained from the General Services Administration, the OMB, and the Office of Personnel Management (OPM).

To conduct this review, we used GAO's *Framework for Assessing the Acquisition Function at Federal Agencies* (September 2005) and DHS' *Acquisition Oversight Program Guidebook* (July 2005) as a baseline. These references identify the following five interrelated elements essential to an efficient, effective, and accountable acquisition process: (1) Organizational Alignment and Leadership, (2) Policies and Processes, (3) Financial Accountability, (4) Acquisition Workforce, and (5) Knowledge Management and Information Systems. We assessed the current status of the acquisition programs by measuring the results of interviews, data analysis, and other relevant documents against critical success factors for these five elements. Overall, the programs and activities we reviewed have made limited or modest progress in areas deemed critical for a fully

successful acquisition program. We determined that significant improvements were needed in all five of the elements identified above. Major concerns for the acquisition programs include: (1) an integrated acquisition system does not exist; (2) full partnership of acquisition offices with other departmental functions has not been realized; (3) comprehensive program management policies and processes are needed; (4) staffing levels and trained personnel are not sufficient; (5) financial and information systems are not reliable or integrated; and (6) timely, corrective actions have not been taken in response to many our and GAO report recommendations.

Our ratings for the acquisition activities we reviewed are based on a four-tiered scale ranging from "Limited Progress" to "Substantial Progress" and are depicted in the following scorecard graphic.

Figure 1: Acquisition Scorecard for Selected DHS Functions



Throughout this report, we depict each of the levels of progress as shown in Figure 2.

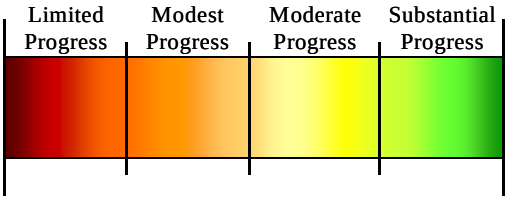
Figure 2: Progress levels for Scorecard Elements

Limited Progress: While there may be plans to address critical success factors, few if any have been implemented.

Modest Progress: While some improvements have been made, many of the critical success factors have not yet been achieved.

Moderate Progress: Many of the critical success factors have been achieved.

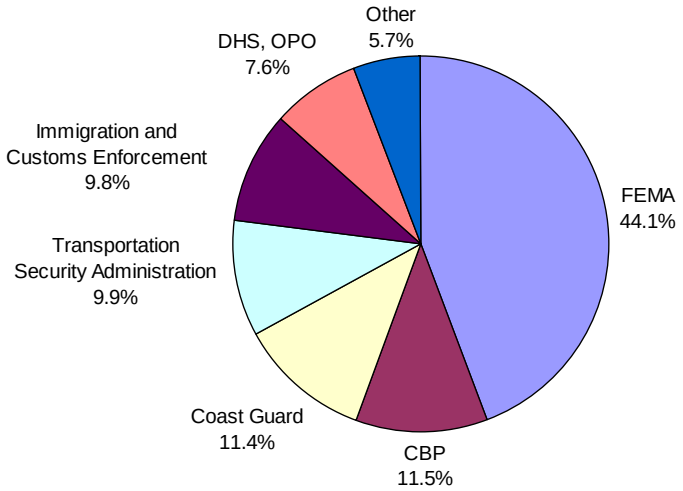
Substantial Progress: Most or all of the critical success factors have been achieved.



The Department of Homeland Security Acquisition Structure

DHS began operations on March 1, 2003. It was created from components of 22 agencies of the federal government. Seven of these legacy agencies, such as FEMA, the USCG, and CBP, retained their own procurement, human resources, finance, and information technology offices and systems. In DHS, these seven procurement offices are called Heads of Contracting Activities. To provide procurement services for the remaining offices of DHS, an eighth office, the Office of Procurement Operations, was created. In FY 2006, the Office of Procurement Operations, FEMA, USCG, and CBP awarded nearly 75 percent of DHS' obligated contracts (see Figure 3).

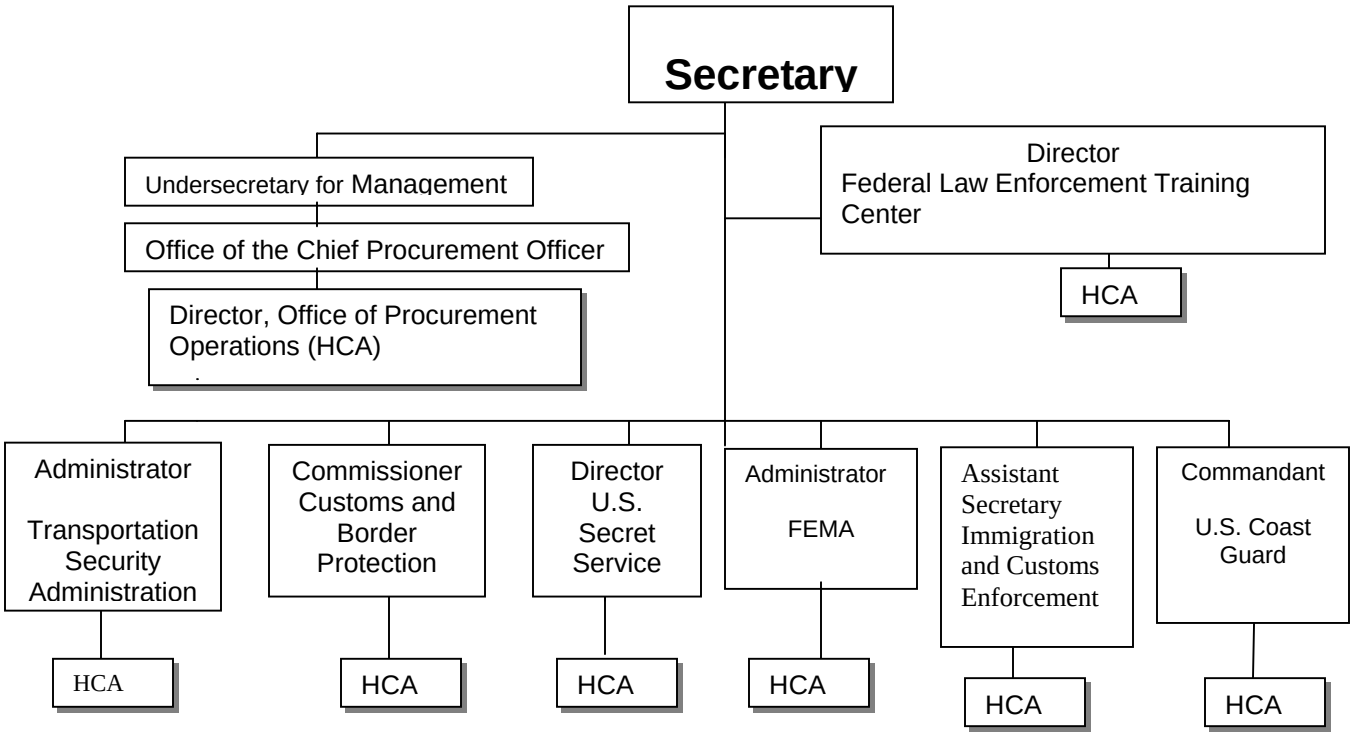
Figure 3: DHS Contracting Obligations by HCA for Fiscal Year 2006
Source: Federal Procurement Data System



<u>Note:</u> FEMA's FY 2006 contract obligations represent a significant increase over the past 2 years due to Hurricane Katrina recovery efforts.

In October 2004, management directives governing acquisitions, human capital, financial management, and information technology were issued, providing that a "Chief" of each of these functions exercise leadership and authority over all aspects of that area within DHS. The acquisition management directive acknowledges the existence of the eight distinct procurement offices, and states that under the concept of dual accountability, each component head shares responsibility for the acquisition function with the DHS Chief Procurement Officer. Additionally, the directive makes clear that the Head of Contracting Activity in each of the eight procurement offices is the individual responsible for the direct management of the entire acquisition function within the component, and reports directly to the component head. See Figure 4 below for Heads of Contracting Activities organization chart.

Figure 4: Organizational Chart Showing the Heads of Contracting Activities in DHS



Source: Office of Inspector General (Based on DHS and Office of Procurement Operations charts)
Notes: (1) Shadowed boxes indicate the eight Heads of Contracting Activities in DHS.
(2) The Office of Procurement Operations provides procurement services for the Office of the Secretary, Citizenship and Immigration Services, the Center for Domestic Preparedness, and numerous other offices.

Structure of the Scorecard

In this report, we reviewed the DHS and FEMA acquisition functions and the acquisition-related activities of two programs, the Integrated Deepwater System Program of the USCG, and SBInet of CBP. Five interrelated elements were used to assess the offices and acquisition-related activities reviewed. The elements are as follows:

- Organizational Alignment and Leadership looks at the placement of the acquisition function in the organization and leadership's support of the function.
- Policies and Processes weigh the adequacy of the rules and practices by which staff carry out the function.
- Financial Accountability determines if systems exist that provide useful, accurate financial information and controls.
- Acquisition Workforce focuses on the numbers and skills of staff needed to effectively and efficiently carry out the function.
- Knowledge Management and Information Systems determines if existing systems provide the data needed to measure performance, provide methods to safeguard assets, and accomplish organizational objectives.

Some examples of critical success factors for each of the elements are as follows: (1) Organizational Alignment and Leadership—ensure appropriate placement of the acquisition function, define and integrate roles and responsibilities, and maintain clear, strong executive leadership; (2) Policies and Processes—partner with internal organizations, use effective project management approaches, and establish effective internal controls; (3) Financial Accountability—partner acquisition management with financial management, integrate financial and operating data, and establish controls and accountability; (4) Acquisition Workforce—commit to human capital management, integrate and align human capital approaches with organizational goals, and target investment in people; (5) Knowledge Management and Information Systems—track key acquisition data, analyze supplies and services spending, and maintain data stewardship. For further information on the elements, see Appendix 1.

ORGANIZATIONAL AND PROGRAM-SPECIFIC PROFILES

DHS' ACQUISITION FUNCTION

The Office of the Chief Procurement Officer is the DHS organization with responsibility for all department acquisition activities and services. This includes management, administration and oversight, financial assistance, and strategic and competitive sourcing.

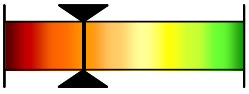
Responsibilities also include the development and publication of department-wide acquisition and financial assistance regulations, directives, policies, and procedures. However, as mentioned previously, each component head shares responsibility for the acquisition function with the DHS Chief Procurement Officer. Therefore, the Chief Procurement Officer has used collaboration and cooperation with the components as the primary means of managing DHS-wide acquisition oversight. Specifically, some of the collaborative methods in use include: integrating the diverse departmental components through common policies and procedures, meeting monthly with Heads of Contracting Activities to discuss issues and to work out problems, and providing input regarding new hires and employee performance for Heads of Contracting Activities staff.

In FY 2006, DHS obligated $15.7 billion in contracts, of which 83 percent was for services. Recent congressional testimony, audits, and reviews cited significant deficiencies in DHS' overall acquisition program, including the following: (1) DHS leadership has not firmly established strong centralized acquisition authority in the Office of the Chief Procurement Officer; (2) DHS has not maintained effective internal control over financial reporting, with recurring significant weaknesses reported; (3) DHS Information Systems are not integrated and do not provide helpful reports and analysis; (4) improvements are needed in the description of technical and performance requirements in contracts; and (5) additional staffing is required for program management activities.

DHS acquisition leaders identified some progress, but significant work remains before the acquisition program is fully functional. While many of the remaining acquisition challenges impact the Office of the Chief Procurement Officer, some of these challenges fall outside of its control. Based on conditions recently disclosed by our office and GAO, interviews with DHS officials, and review of data, we rated the five interrelated elements essential to an efficient and effective acquisition process. These ratings reflect the performance or capabilities of the acquisition function. The ratings and a brief summary of each element are discussed below.

Organizational Alignment and Leadership

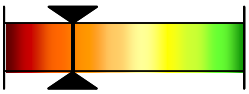
Modest Progress



DHS' executive leadership has made modest progress in ensuring the acquisition program achieves the organizational alignment needed to perform its functions. One area of improvement reported by interviewees was the increased communication by acquisition leadership to inform staff about the role and importance of their mission to DHS. The atmosphere for collaboration between DHS and its component agencies on acquisition matters has also improved.

Important problems still exist in this area, however. Deficiencies previously reported by our office and GAO are largely uncorrected in critical areas necessary for effective

acquisition organizations. The acquisition program continues to be viewed by many as a support function (i.e., contract processing office) instead of a partner. Furthermore, acquisition management has only recently begun receiving sufficient resources from DHS leadership for adequate staffing and training. Strong executive leadership is needed to ensure that the importance of the acquisition function is acknowledged and integrated with all other functions involved in, or affected by, procurement activities.

Policies and Processes Modest Progress 

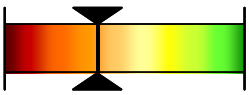
DHS has made modest progress in developing policies and processes to ensure components comply with regulations, policies, and processes to achieve department-wide goals. In 2005, a management directive, accompanied by the *Acquisition Oversight Program Guidebook*, established policies and procedures for oversight of DHS acquisitions, with the common goal of delivering mission results while maintaining compliance with applicable laws, regulations, policies, and procedures. An acquisition manual and additional acquisition regulations for DHS have also been developed.

According to GAO and our recent reports and interviews with DHS officials, the need still remains for a comprehensive DHS approach to program management standards. Across various parts of DHS, expediency and poorly defined requirements have caused problems for the department's acquisition efforts.

Financial Accountability Limited Progress 

DHS has made limited progress in ensuring that there is financial oversight and accountability within the acquisition function. Our interviews, review of prior reports, and relevant data have indicated that DHS financial information is generally unreliable, and that the financial systems do not have the internal controls and integration that acquisition personnel require. Also, the acquisition and finance offices have not successfully partnered on acquisition planning and strategic decision making.

From our interviews, we determined that there were numerous and persistent issues with inadequate internal controls and data verification. Improper payments have been made, and there are few checks on data once it is inputted into the system. This problem is exacerbated by the use of multiple, nonintegrated information technology systems across the department. Without a reliable data system, it has been very difficult for the financial office to make an impact in the broader acquisition process.

Acquisition Workforce Modest Progress 

DHS has made modest progress in building a skilled acquisition workforce. An increase in the personnel budget has allowed DHS to fill many needed acquisition staff positions.

However, until a fully trained acquisition workforce is developed, it will be difficult to achieve further progress needed for an efficient, effective, and accountable acquisition function.

In previous reports, our office and GAO identified the need for additional certified program managers. The Office of the Chief Procurement Officer subsequently created a Program Management training program that should greatly increase the pool of certified program managers. Additional training and personnel are necessary, however, to reach an adequate number of certified program managers.

Interviewees expressed concern that the acquisition organization was "top heavy," with too many senior grade level personnel. Data from OPM indicates that more than 40 percent of DHS' contracting officers will be eligible to retire in the next 5 years. To counteract these problems, DHS plans to use additional appropriations to hire more personnel and implement an acquisition internship program that will bring in junior staff. The results of these efforts are not yet apparent.

Knowledge Management and Information Systems Limited Progress 

DHS has made limited progress in developing and deploying information systems to track and analyze acquisition data, and improve user efficiency. Current systems are not fully integrated, contain unreliable input, and do not have internal controls to verify data. As a result, the acquisition program cannot effectively provide information to all of its stakeholders and does not have the tools necessary to perform analysis for planning or monitoring its transactions.

Previous reports found that many DHS components still maintained their legacy contract writing systems, and that a need for integration between contract writing and contract management systems increased the risk of data error. DHS has selected PRISM as its standard contract writing system, but the department-wide rollout is behind schedule. Integration and data accuracy problems will continue to exist until all components migrate to the same contract writing system.

FEMA's Acquisition Function

FEMA is the primary federal agency that leads the United States in preparing for, preventing, responding to, and recovering from disasters. FEMA's mission includes: (1) maintaining preparedness of emergency response personnel throughout the United States; (2) providing logistical support for disaster mitigation and recovery efforts; (3) disbursing funds for rebuilding required as a result of a disaster; and (4) providing relief for individual citizens and businesses. FEMA coordinates the response to disasters that

would otherwise overwhelm the resources of state and local authorities. FEMA's Office of the Chief Acquisition Officer provides acquisition services and solutions to support the agency's mission.

For FY 2006, FEMA obligated $7 billion in contracts, of which 89 percent was for services. FEMA spent $6.2 billion in services, such as construction/family housing, and $727 million for goods, such as trailers and plastic fabricated materials.

Organizational Alignment and Leadership Limited Progress

Executive leadership has made limited progress toward partnerships among various functional departments, and in aligning FEMA's acquisition function with DHS' mission and needs. The agency's acquisition office is viewed more as a support function than as a partner, and it is not aligned organizationally to ensure efficiency and accountability. The actions taken by DHS have been too few and the process too slow to ensure that FEMA's acquisition function will meet the department's goals.

GAO and we cite significant deficiencies and concerns related to FEMA's organizational alignment and leadership. In March 2006, we disclosed that FEMA had reorganized its divisions and offices five times since 1995. In February 2007, the Inspector General testified that a need for clear lines of acquisition authority among states, local, and federal authorities contributed to the poor response to Hurricane Katrina. While we cited improvements in FEMA's overall acquisition capability, concerns remain about acquisition planning for a catastrophic disaster.

We interviewed FEMA acquisition leaders. They provided several examples of progress, such as the creation of the Acquisition Business Office to assist with strategic planning, and the establishment of a Project Integration System, which will create teams consisting of staff from different offices to draw up acquisition proposals. Additional positive signs include the restructuring of two Heads of Contracting Activities into one, and the development of the new Acquisition Tracker, to monitor status of all acquisitions from beginning to end.

Remaining significant issues include the need for more funding and staffing, especially for strategic planning. Internal reviews of management structure need to be completed so that improvements can be implemented. Also, acquisition personnel are frequently left out of key decisions, sometimes leading to "buying the wrong thing quickly." Finally, the Acquisition Business Office is not yet recognized in FEMA's financial system, and therefore has no money for travel or training.

Policies and Processes Limited Progress 

DHS and FEMA have made limited progress in developing adequate policies and processes to ensure that FEMA can efficiently and effectively perform the acquisition function. FEMA has not formed the necessary relationship with stakeholders to analyze agency needs and ensure goods and services are delivered according to the contract terms.

Interviews with FEMA acquisition leaders established that progress has been made in the following areas: an increase in readiness contracts; the development of a Contract Management Guide to assist new employees; and the creation of an Emergency Acquisition Field Guide to assist disaster response staff. FEMA has exceeded agency goals for procurements from small businesses and drafted a new set of FEMA policies and procedures for acquisitions.

Remaining significant issues are insufficient program management and oversight, increasing the risk of waste, fraud, and abuse, and the need for an automated system or checklist for identification of high-risk contracts. Outdated policies and limited training for staff using the Emergency Acquisition Field Guide are additional concerns.

Financial Accountability Limited Progress 

Limited progress has been made to ensure that FEMA has adequate financial accountability within its acquisition function. Agency management believes that FEMA's financial systems hinder strategic planning and contract administration. Our prior reports have disclosed a need for internal controls and proper accounting. An October 2006 summary report found inappropriate award of contracts and the need to inspect deliverables before acceptance and payment. One month later, we said that FEMA did not have disaster contract information readily available and the agency was unable to fully support the accuracy and completeness of $22.3 billion in unpaid obligations and $1.5 billion in accounts payable. In February 2007 testimony, FEMA was cited for problems in issuing, monitoring, and closing mission assignments.

In interviews with FEMA acquisition leaders, the new Acquisition Tracker, which includes data from the procurement, program, and finance offices, was seen as an important first step to integrate FEMA's finance and acquisition offices. Unfortunately, current financial systems do not have important analytical capabilities and FEMA does not have an information technology strategy for integrating financial and acquisition management data. Several other remaining significant issues included immature partnerships between FEMA offices with acquisition functions, frequently irrelevant or unusable financial reports, and incomplete assessments of payment accuracy.

Acquisition Workforce

Limited Progress 

FEMA has made limited progress in developing the necessary acquisition workforce, and it continues to experience problems with fully staffing its acquisition office and giving the workforce necessary skills and training. A November 2006 report found that the acquisition staff in FEMA were improperly trained and too small to oversee the large number of Katrina-related contracts, and prevent fraud, waste, and abuse. In February 2007 testimony, the Inspector General said the need for acquisition staff continues to hamper FEMA's overall disaster response efforts.

FEMA acquisition leaders have plans for improvements in this area, including a formal process for reviewing and adjusting workloads, the creation of a Strategic Workforce Plan, and the development of an Acquisition Intern Program. Moreover, steps have been taken to expedite hiring, align performance plans with FEMA's goals, and measure acquisition effectiveness and efficiency.

Unfortunately, further work is needed on many issues, including finalizing the Strategic Workforce Plan, which remains in draft form. Further work is also needed to decrease the length of the hiring process, improve FEMA's image in order to attract staff, and decrease attrition in an office where half of the contracting officers will be eligible to retire over the next 5 years.

Knowledge Management and Information Systems

Limited Progress 

DHS and FEMA have made limited progress in ensuring that the acquisition function has the necessary tools in its knowledge management and information systems. Information technology systems are not meeting the needs of the acquisition management function, and while a need for improvement is widely recognized, FEMA leadership and acquisition personnel disagree on the best way to rectify these deficiencies.

Previous review and audits have identified several problems with FEMA's information technology systems. Our November 2006 report said that FEMA's National Emergency Management Information System was unable to compare actual purchases in the field to the maximum amount authorized. In January 2007, a FEMA contractor performed an independent assessment and reported that FEMA had no clearly communicated information technology strategy. Another report said that FEMA's information technology tools were deficient, outdated, or nonexistent.

We interviewed FEMA acquisition leaders who believe that use of the PRISM contract writing system throughout FEMA, beginning in February 2008, will be a positive development. Currently, the use of several outdated and nonintegrated systems

frequently requires manual data input from one system to another. Also, systems are not user friendly and training is inadequate. Interviewees also reported a need for internal controls to ensure data accuracy.

United States Coast Guard Deepwater Program

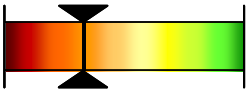
The Integrated Deepwater System Program (Deepwater) is a $24 billion, 25-year acquisition program designed to replace, modernize, and sustain the USCG's aging and deteriorating fleet of ships and aircraft. The Deepwater acquisition strategy uses a non-traditional system-of-systems approach in which private industry was asked to develop and propose an optimal mix of assets, infrastructure, information systems, and people solutions designed to accomplish Deepwater's missions. Additionally, the private sector was to provide the assets, the systems integration, integrated logistics support, and program management. Between FYs 2001 and 2007, Deepwater was allocated more than $4 billion, or 66 percent of the USCG's Acquisition, Construction, and Improvements budget.

Over the past year, a number of audits, studies, and internal reviews were conducted on the Deepwater program. These reviews identified management challenges and risks that include: (1) inadequate definition, understanding, and stability of requirements; (2) excessive reliance on the system integrator to manage the Deepwater program; (3) inability to properly assess programmatic risk; (4) need for expertise in cost estimation; (5) Deepwater program management did not easily adapt to the environment of changing missions and requirements, and major systems integration; and (6) a Deepwater acquisition workforce that does not have the requisite training, experience, certification, and structure to acquire assets and systems of significant scope and complexity.

To its credit, the USCG recognizes that urgent and immediate changes are needed in its management of major acquisitions. For example, the USCG recently issued its *Blueprint for Acquisition Reform* (Blueprint), which catalogs and proposes solutions to many of the aforementioned challenges that have historically impeded the execution of Deepwater projects. According to the USCG, implementing the Blueprint will enhance its ability to execute asset-based traditional projects, effectively employ a governmental or commercial entity as a systems integrator for complex acquisitions, and efficiently execute non-major acquisitions for necessary goods and services.

Based on conditions disclosed by our office and other independent reviews, and discussions with USCG personnel, we rated the five interrelated elements essential to an efficient and effective acquisition process. These ratings reflect the performance or capabilities of the acquisition process. The ratings and a brief summary of each element are discussed below.

Organizational Alignment and Leadership Modest Progress



USCG leadership has made modest progress in ensuring it achieves the organizational alignment needed to perform its acquisition functions. One sign of progress was the re-establishment of a single USCG acquisition structure, after the creation of a separate Deepwater acquisition structure proved problematic.

Significant changes to the USCG's acquisition organization are necessary to successfully merge the two acquisition components, both structurally and culturally. In its Blueprint, the USCG has identified action items that it plans to implement in order to improve its Deepwater program. These include: (1) ensuring overarching roles and responsibilities of the acquisition function and acquisition personnel are well defined; (2) incorporating the Heads of Contracting Activities into the consolidated acquisition structure; (3) determining measures that assess the health of the acquisition function; and (4) expanding and building upon existing USCG surveys to solicit views on the effectiveness of communications, effectiveness of acquisition processes, and areas needing improvement.

Policies and Processes Limited Progress

USCG leadership has made limited progress in ensuring it establishes the policies and processes needed to perform acquisitions effectively and efficiently. It is notable that, in advance of Blueprint implementation, the USCG has taken key steps toward improving Deepwater program management and contractor oversight, including: (1) issuing a Commandant's Instruction reaffirming the Assistant Commandant for Systems as the USCG's "Technical Authority" for all acquisition projects; (2) revising Deepwater contract award terms to more accurately and objectively reflect past contractor performance; and (3) establishing a Risk Management Board to support a comprehensive approach to determining, assessing, documenting, and mitigating programmatic risks.

However, USCG recognizes that it must take further action to establish and strengthen policies and processes for its realigned acquisition function. In its Blueprint, USCG has identified action items that it plans to implement. They include updating the Major Systems Acquisition Manual to reflect collaborative requirements process, systems program management, acquisition strategy process, and conducting independent verification and validation of cost, schedule, and performance measurement baselines for major systems. The USCG also plans to institute third-party, independent programmatic assessments, determining technical maturity, and verifying design stability, while also ensuring that any modifications to the Deepwater contract for the performance period

beginning in June 2007 will sufficiently support improved program management and increased contractor oversight.

Financial Accountability Limited Progress 

USCG leadership has made limited progress in ensuring its acquisition function achieves the financial accountability needed to perform efficiently. It must address issues raised in the Defense Acquisition University review of the Deepwater program.

This review identified financial accountability as a special interest area. It reported that: (1) Deepwater financial management is distributed to a number of offices and individuals, and that no one person is responsible for oversight of financial planning; (2) the USCG does not routinely conduct independent third-party cost estimates; (3) there are an inordinate number of requirements changes and undefinitized contract actions; (4) Deepwater decisions were not supported or needed business case studies; (5) the USCG needed flexibility in the reprogramming of funds during execution; and (6) the USCG does not routinely develop independent life cycle cost estimates.

In its Blueprint, the USCG has identified action items that it plans to implement in order to improve its Deepwater program. These include: (1) integrating all three USCG accounting systems into a complete data set useable by all acquisition personnel; (2) developing business cases in support of all key Deepwater acquisition decisions; (3) developing an independent third-party cost estimates for the Deepwater Program; and (4) reducing the number of requirements changes and undefinitized contract actions.

Acquisition Workforce Limited Progress 

USCG leadership has made limited progress in ensuring it has the numbers and skills of acquisition workforce needed to support Deepwater acquisitions. The USCG has taken the first steps to revitalize its acquisition workforce. It is currently finalizing almost every acquisition position description to ensure the right personnel with the best skills are properly placed into the right acquisition positions, as needed to aid program success. It has added Deputy Program Manager positions to the various acquisition domains, and it has begun filling these positions with Senior Executive Service and General Schedule 15 level personnel, to build continuity into the acquisition program.

However, USCG has serious concerns regarding the size and capabilities of the acquisition workforce handling the Deepwater major systems acquisitions. Recently, the Defense Acquisition University reported the USCG does not possess a sufficient number of acquisition personnel with training, major acquisition experience, and certifications to properly manage the Deepwater program. It also reported that the three major acquisition

areas in greatest need of an infusion of experience are program management, contracting, and financial management.

In its Blueprint, USCG has identified action items that it plans to implement in order to improve its Deepwater program. These plans include: (1) developing and implementing a comprehensive long-range Strategic Workforce Plan; (2) recruiting, hiring, and retaining experienced and certified acquisition professionals in program management (military), contracting (civilians), and other required acquisition career fields; (3) determining and applying creative pay, recruitment, retention, and other incentives to entice and retain qualified, experienced acquisition personnel; and (4) transitioning or developing specific individual acquisition skills through training, education, and internships.

Knowledge Management and Information Systems — Limited Progress

USCG leadership has made limited progress in ensuring it has the knowledge management and information systems needed to perform its acquisition functions. The GAO and the Defense Acquisition University have both reported concerns with the reliability and accuracy of USCG's Deepwater program Earned Value Management System and Integrated Master Schedule information management systems. These information management systems are intended to help Deepwater program managers make well-informed programmatic decisions and exercise oversight of the Deepwater contract.

However, both the GAO and the Defense Acquisition University have reported that these management systems were not properly maintained and therefore impaired the Coast Guard's ability to effectively manage the Deepwater program. The Defense Acquisition University reported that the earned value metrics used in the Deepwater program neglected to determine trends or highlight re-baselines.

The GAO reported in June 2004 that USCG was only maintaining the schedules of individual assets at the lowest, most detailed level and not at the integrated level. The need for an accurate integrated acquisition schedule for the Deepwater program was a symptom of larger issues that they had raised questioning whether the Deepwater acquisition was being properly managed and the government's interest was being safeguarded.

In its Blueprint, USCG has identified action items that it plans to implement in order to improve its Deepwater program. These planned items include: (1) implementing Earned Value Management on all required acquisition projects according to DHS requirements; (2) developing metrics to assess the effectiveness of the acquisition function for major systems; (3) developing an Acquisitions Directorate Integrated Master Plan and

Integrated Master Schedule for all projects and to track status; and (4) developing key financial/schedule/Earned Value Management reports and provide training for all program and project managers.

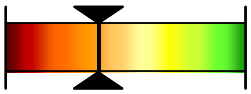
Customs and Border Protection SBInet Program

Secure Border Initiative Network Program

The Secure Border Initiative (SBI) was created in September 2005 to provide a comprehensive approach to border security and illegal immigration. A portion of CBP efforts focus on a major systems acquisition program to modernize border patrol operations, called SBInet. The SBInet program is charged with developing and installing the technology and tactical infrastructure solutions to gain effective control or our Nation's borders. In September 2006, CBP competitively awarded a systems integration contract for SBInet to the Boeing Company and is planning additional contract actions.

In FY 2006, CBP was provided $325 million in supplemental funding for tactical infrastructure and technology. With the subsequent SBInet program initiation, Congress appropriated $1.2 billion in the CBP Border Security, Fencing, Infrastructure, and Technology appropriation for FY 2007. However, Congress withheld $950 million of the FY 2007 appropriation contingent upon approval of the FY 2007 SBInet Expenditure Plan. On March 22, 2007, the House of Representatives approved the release of $405 million of the withheld funds. The Senate has not commented on the FY 2007 SBInet Expenditure Plan. The FY 2008 President's Budget requests an additional $1 billion to fund the SBI Program offices, the operations and maintenance of new and legacy equipment, and to continue to develop and deploy SBInet solutions for technology and tactical infrastructure, as well as the common operation picture.

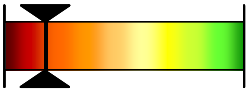
Organizational Alignment and Leadership — Modest Progress



The organizational structure has the SBInet Systems Program Office[3] (SPO) reporting to a SBI Program Executive Office (PEO). The PEO reports directly to the CBP Commissioner's office. While this organizational structure now closely resembles the recommendations of a contracted staffing study completed in December 2006[4], the SBInet program's organization structure has been unstable and evolving. In March 2006, CBP reorganized the Procurement Directorate to commit procurement specialists to the planning of SBInet acquisitions. The new SBI Acquisition Office reports directly to the CBP Chief Financial Officer and has its own Heads of Contracting Activities. We will continue to monitor the evolving organization structure to assess whether procurement

[3] Also referred to as SBInet Program Management Office (PMO).
[4] Homeland Security Institute, *Secure Border Initiative Staffing Analysis*, December 2006.

specialists are properly included in acquisition planning. In addition, CBP created the Executive Steering Council to provide senior management oversight of the SBI program. However, gaps remain among program management, planning, and contract administration. Further, CBP faces challenges overcoming cultural change and improving planning and acquisition through cooperation, teamwork, and defined roles and responsibilities.

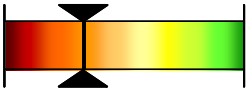
Policies and Processes Limited Progress 

CBP did not have a pre-existing program management workforce to establish, implement, and refine SBInet policies and processes. The SBInet SPO had to create staffing plans, locate workspace, and establish business processes while simultaneously initiating one of the largest acquisition programs in the department. The SBInet SPO has begun identifying and generating program management policies and processes and recently created a Process Library to communicate program management polices and processes. In addition, the Executive Steering Council meets frequently and communicates lessons learned from CBP's other major systems acquisition programs.

DHS has a Memorandum of Understanding with the Defense Contract Audit Agency (DCAA) for audit services. Interagency Agreements were issued for audits of cost incurred on future Cost-Reimbursable Tasks Orders and Cost/Price Proposals. However, a planned interagency agreement with the Defense Contract Management Agency to provide contract oversight services at The Boeing Company facilities is not in place.

The SBInet SPO has not finalized an acquisition program baseline to establish program cost, schedule, and technical performance goals from which to gauge progress. Further, an EVMS to measure program and contractor performance was not operating because a performance management baseline has not been finalized.

On March 6, 2007, CBP created the SBI Acquisition Office to enhance upfront communications with the SBInet SPO and to administer SBI-related acquisitions, including SBInet. The SBI Acquisition Office adheres to the Federal Acquisition Regulation, DHS Acquisition Regulation, and CBP policies and processes administered by the CBP Procurement Directorate. However, acquisition planning and program management systems and processes need improvement. Additionally, roles and responsibilities under the new office have not been clarified.

Financial Accountability Modest Progress 

New legislative mandates and policy direction required the use of FY 2007 appropriations to accelerate fence-building projects and to begin addressing Northern Border vulnerabilities. At the SBInet program initiation in FY 2006, CBP used

supplemental funds and the CBP Salaries and Expenses appropriation to fund program start-up. The House of Representatives continues to withhold $545 million of the FY 2007 appropriation contingent upon CBP's demonstration of how the SBInet program will achieve a certain, defined, and measurable level of border control. The Senate has not provided comment on the FY 2007 SBInet Expenditure Plan. Progress in meeting SBInet mission needs is contingent upon the release of the $950 million withheld from the FY 2007 appropriation and upon the continued funding of the program through FY 2011.

CBP uses Systems Applications Products (SAP) and the Intelligent Procurement System (IPRO) to record and manage budgets and expenditures. These systems provide key functionality for financial management of major systems acquisition program. The IPRO facilitates contract writing and records obligations, and SAP provides tools to display obligations and expenditures graphically, which is useful for gauging contractor progress. However, the latter product has limited interface with the DHS Federal Procurement Data System Next Generation, requiring information transferred to be manually verified for accuracy.

Acquisition Workforce Limited Progress 

In November 2006, we reported that the department did not have the capacity to effectively plan, oversee, and execute the SBInet program; administer its contracts; and control costs and schedule. The SBInet SPO has made significant progress since November. For example, the department conducted an independent study[5] of the organization and staffing needs for the program, and CBP has implemented an organizational structure that closely reflects the study's recommendations. The PEO consisted of approximately 25 positions and the SBInet SPO consisted of approximately 124 positions. However, additional staff with the requisite skills are needed to perform analysis of alternatives, prepare and administer task orders, and manage contractor cost, schedule, and performance. Furthermore, CBP does not have a performance-based rating system to link performance with organizational goals and SBInet does not have a Human Capital Plan.

Filling the positions in the SBInet organizational structure has been and continues to be a difficult challenge, which adversely affects the program. The transfer of 14 positions originally assigned to the CBP Procurement Directorate comprised the SBI Acquisition Office. Five Procurement Directorate specialists supplemented the SBI Acquisition Office staff on a part-time basis. The PEO was recruiting personnel to fill 26 positions and the SBInet SPO was recruiting to fill 235 positions. The SBI Acquisition Office was also actively recruiting to fill 17 positions concurrently with the Procurement Directorate's attempts to fill 50 contract and acquisition specialist positions. On-board

[5] Homeland Security Institute, *Secure Border Initiative Staffing Analysis*, December 2006.

staff, while focused and motivated, have unsustainable workloads. While SBInet officials assert sufficient staff are on-hand to administer the four task orders issued, more contract actions are planned. Moreover, as a result of unfilled positions, work on tasks for major systems acquisition programs, especially the analysis of alternative solutions and logistics support analysis and planning, which are key to managing and reducing lifecycle costs, is deferred. The SBInet program's ambitious schedule of work planned for summer 2007 will exceed the staff's capacity to manage the program without significant staff increases.

Knowledge Management and Information Systems

Limited Progress

The SBInet SPO used electronic-Program Management Office System (*ePMO),* a government off-the-shelf management information system, to record deliverables, track program documentations, and support document flow through development, review, and approval processes. The SBI Acquisition Office was able to access *ePMO*. However, *ePMO* does not interface with other DHS systems, and CBP does not have a knowledge management system. The SBInet program uses two automated systems to collect procurement data. SAP is used to record and access financial information and IPRO is used to generate contract documents and track basic procurement data such as requisition numbers, obligations, and the date of contract awards. However, SAP and IPRO information uploaded to Federal Procurement Data System Next Generation must be manually verified for accuracy. In addition, the Boeing Company was not providing cost, schedule, and performance data to the Earned Value Management Reports to help the SBInet SPO exercise oversight of the program.

Scorecard - Appendix 1
Elements of an Efficient, Effective, and Accountable Acquisition Process

Organizational Alignment and Leadership. The end goal of organizational alignment is to ensure that the acquisition function enables the agency to meet its overall mission and needs. The acquisition function needs proper management support and visibility within the organization to meet that goal. Leaders have the responsibility to set the corporate agenda, define and communicate the organization's values and culture, and remove barriers that block organizational change.

Policies and Processes. Policies and process embody the basic principles that govern the way an agency performs the acquisition function. Planning strategically requires determining and managing relationships of those involved in the acquisition process, analyzing aggregate agency needs, and devising strategic acquisition plans to meet those needs. Agency processes need to ensure that contracted goods and services will be delivered according to the schedule, cost, quality, and quantity specified in the contract.

Particular attention should be given to capital investments since they require more analysis, support, and review than projects that cost less, have shorter timeframes, or have less agency-wide impact.

Financial Accountability. Sound financial systems provide credible, reliable, and accurate information that can: (1) ensure that the agency meets its financial obligations, (2) enhance strategic acquisition decisions, and (3) enable effective evaluation and assessment of acquisition activities.

Acquisition Workforce. Successful acquisition efforts depend on agency and management valuing and investing in the acquisition workforce. By focusing on hiring, training, and professional development, strategic planning outlines ways to help fill gaps in knowledge, skill, and abilities. Sufficient attention needs to be given to acquiring, developing, and retaining talent or federal agencies could lose a significant portion of their contracting knowledge base. Leading organizations foster a work environment in which people are empowered and motivated to contribute to continuous learning and mission accomplishment.

Knowledge Management and Information Systems. Leading organizations gather and analyze data, generally through information systems, to identify opportunities to reduce cost, improve service, measure compliance, and provide better management. Data collected in support of meaningful metrics can assist agencies to track achievement of plans, goals, and objectives and to analyze the differences between actual performance and planned results. However, it is essential that acquisition management systems contain appropriate, cost-effective controls to: (1) safeguard assets, (2) ensure accurate aggregation and reporting of information, and (3) support the accomplishment of organizational objectives. Appropriate and cost-effective controls provide accessible, timely, and accurate data to managers and others needing acquisition information.

APPENDICES

Appendix 1
Audit Reports With Questioned Costs

Report Category	Number	Questioned Costs	Unsupported Costs
A. Reports pending management decision at the start of the reporting period	139	$211,336,209	$76,096,432
B. Reports issued/processed during the reporting period with questioned costs	31	$53,328,190	$6,168,625
Total Reports (A+B)	170	$264,664,399	$82,265,057
C. Reports for which a management decision was made during the reporting period	17	$28,676,159	$0
(1) Disallowed costs	4	$8,900,000	$0
(2) Accepted costs	13	$19,776,159	$0
D. Reports put into appeal status during period	0	$0	$0
E. Reports pending a management decision at the end of the reporting period	153	$235,988,240	$82,265,057
F. Reports for which no management decision was made within six months of issuance	122	$182,660,050	$76,096,432

Notes and Explanations:

Management Decision - occurs when DHS management informs us of its intended action in response to a recommendation and we determine that the proposed action is acceptable.

Accepted Costs - are previously questioned costs accepted in a management decision as an allowable cost to a government program. Before acceptance, we must agree with the basis for the management decision.

In Category C, lines (1) and (2) do not always equal the total on line C because resolution may result in values greater than the original recommendations.

Questioned costs – Auditors commonly question costs arising from an alleged violation of a provision of a law, regulation, grant, cooperative agreement or contract. A "questioned" cost is a finding in which, at the time of the audit, is not supported by adequate documentation or is unreasonable or unallowable. A funding agency is responsible for making management decisions on questioned costs, including an evaluation of the findings and recommendations in an audit report. A management decision against the auditee would transform a questioned cost into a disallowed cost.

Unsupported costs - are costs that are not supported by adequate documentation.

Appendix 1b
Audit Reports With Funds Put to Better Use

Report Category	Number	Amount
A. Reports pending management decision at the start of the reporting period	11	$63,463,672
B. Reports issued during the reporting period	3	$1,329,074
Total Reports (A+B)	14	$64,792,746
C. Reports for which a management decision was made during the reporting period.	1	$860,000
(1) Value of recommendations agreed to by management	1	$860,000
(2) Value of recommendations not agreed to by management	0	$0
D. Reports put into the appeal status during the reporting period	0	$0
E. Reports pending a management decision at the end of the reporting period.	13	$63,932,746
F. Reports for which no management decision was made within 6 months of issuance	10	$62,603,672

Notes and Explanations:

In category C, lines (1) and (2) do not always equal the total on line C since resolution may result in values greater than the original recommendations.

Funds Put to Better Use – Audits can identify ways to improve the efficiency, effectiveness, and economy of programs, resulting in costs savings over the life of the program. Unlike questioned costs, the auditor recommends methods for making the most efficient use of federal dollars, such as reducing outlays, deobligating funds, or avoiding unnecessary expenditures.

Appendix 2
Compliance – Resolution of Reports and Recommendations

MANAGEMENT DECISION IS PENDING

9/30/06	
Reports open over 6 months	216
Recommendations open over 6 months	989
3/31/07	
Reports open over 6 months	199
Recommendations open over 6 months	986

CURRENT INVENTORY

Open reports at the beginning of the period	404
Reports issued this period[1]	158
Reports closed this period	99
Open reports at the end of the period	463

ACTIVE RECOMMENDATIONS

Open recommendations at the beginning of the period	1,688
Recommendations issued this period	550
Recommendations closed this period	196
Open recommendations at the end of the period	2,042

Notes and Explanations:

[1]Includes 20 management audit reports issued from our Office of Audits, 7 management audit reports issued from our Office of Information Technology-Audits, 3 management audit reports issued from our Office of Inspections, 6 management audit reports issued from our Office of Disaster Assistance Oversight (DAO), 16 grant audit reports issued from our DAO, 49 Defense Contract Audit Agency reports processed by our Office of Audits, and 57 single audit reports processed by our Office of Audits.

Appendix 3
Management Reports Issued

	Program Office/Report Subject	Report Number	Date Issued
1.	Treatment of Immigration Detainees Housed at Immigration and Customs Enforcement Facilities	OIG-07-01	12/06
2.	The State of North Carolina's Management of State Homeland Security Grants Awarded During Fiscal Years 2002 and 2003	OIG-07-02	10/06
3.	Management Advisory Report on the Condition, Losses, and Possible Uses of FEMA Modular Housing	OIG-07-03	10/06
4.	Allegations Regarding San Francisco International Airport	OIG-07-04	10/06
5.	Federal Protective Service Needs to Improve its Oversight of the Contract Guard Program	OIG-07-05	10/06
6.	Federal Emergency Management Agency's Public Assistance Grant Funds Awarded to the Macon Water Authority After Tropical Storm Alberto	OIG-07-06	11/06
7.	Risk Management Advisory for the SBInet Program Initiation	OIG-07-07	11/06
8.	U.S. Immigration and Customs Enforcement's Detainee Tracking Process	OIG-07-08	11/06
9.	Targeting Oceangoing Cargo Containers *(Unclassified Summary)*	OIG-07-09	11/06
10.	Independent Auditors' Report on DHS' FY 2006 Financial Statements (Excerpts from the DHS Performance Accountability Report)	OIG-07-10	11/06
11.	U.S. Citizenship and Immigration Services' Progress in Modernizing Information Technology	OIG-07-11	11/06
12.	Major Management Challenges Facing the Department of Homeland Security (Excerpts from the FY 2006 DHS Performance and Accountability Report)	OIG-07-12	12/06
13.	DHS' Corrective Action Plan Process for Financial Reporting – Report No. 3	OIG-07-13	12/06

Appendix 3
Management Reports Issued

	Program Office/Report Subject	Report Number	Date Issued
14.	Improvements Needed in TSA's Federal Flight Deck Officer Program *(Unclassified Summary)*	OIG-07-14	12/06
15.	Implementation Challenges Remain in Securing DHS Components' Intelligence Systems *(Unclassified Summary)*	OIG-07-15	12/06
16.	Improved Administration Can Enhance U.S. Customs and Border Protection Laptop Computer Security *(Redacted)*	OIG-07-16	12/06
17.	FEMA's Progress in Addressing Information Technology Management Weaknesses	OIG-07-17	12/06
18.	Information Technology Matters Related to TSA's FY 2005 Financial Statements *(Redacted)*	OIG-07-18	12/06
19.	Independent Auditors' Report on CBP's FY 2006 Consolidated Financial Statements (Excerpts from the CBP Performance and Accountability Report)	OIG-07-19	12/06
20.	DHS' Internal Control Over Financial Reporting – FY 2006	OIG-07-20	12/06
21.	FEMA Internal Controls for Funding Administrative Cost under State Management Grants	OIG-07-21	1/07
22.	DHS' Management of BioWatch Program	OIG-07-22	1/07
23.	Acquisition of the National Security Cutter, U.S. Coast Guard	OIG-07-23	1/07

Appendix 3
Management Reports Issued

	Program Office/Report Subject	Report Number	Date Issued
24.	DHS' Implementation of Protective Measures for Personally Identifiable Information *(Redacted)*	OIG-07-24	1/07
25.	Technical Security Evaluation of DHS Activities at Dulles International Airport *(Unclassified Summary)*	OIG-07-25	1/07
26.	Federal Emergency Management Agency Public Assistance Grant Funding Awarded to the City of Richmond California After the Loma Prieta Earthquake	OIG-07-26	2/07
27.	110'/123' Maritime Patrol Boat Modernization Project, United States Coast Guard	OIG-07-27	2/07
28.	ICE's Compliance with Detention Limits for Aliens With a Final Order of Removal From the United States	OIG-07-28	2/07
29.	DHS' Corrective Action Plan Process for Financial Reporting – Report No. 4	OIG-07-29	2/07
30.	Follow up on Recommendations from Audit of Procedures to Detect Uranium in Two Smuggling Incidents *(Unclassified Summary)*	OIG-07-30	2/07
31.	Special Transient Accommodations Program for the Evacuees From Hurricanes Katrina and Rita	OIG-07-31	2/07
32.	Customs and Border Protection's Agriculture Inspection Activities	OIG-07-32	2/07
33.	The Department of Homeland Security's Role in Food Defense and Critical Infrastructure Protection	OIG-07-33	2/07
34.	An Assessment of United States Immigration and Customs Enforcement's Fugitive Operations Teams	OIG-07-34	3/07
35.	Access to Airport Secured Areas *(Unclassified Summary)*	OIG-07-35	3/07
36.	FEMA's Award of 36 Trailer Maintenance and Deactivation Contracts	OIG-07-36	3/07

Appendix 4
Financial Assistance Audit Reports Issued

	Report Number	Date Issued	Auditee	Questioned Costs	Unsupported Costs	Funds Put to Better Use
1.	DA-07-01	10/06	Emergency Management Performance Grant Funds Awarded to the Virgin Islands Territorial, Emergency Management Agency	$190,877	$0	$0
2.	DA-07-02	10/06	Hurricane Katrina Activities, City of Gulfport, Mississippi	$0	$0	$0
3.	DA-07-03	11/06	Virgin Islands Water and Power Authority	$8,659	$0	$0
4.	DA-07-04	11/06	Hurricane Wilma Activities, City of Port Saint Lucie, Florida	$447,116	$0	$0
5.	DA-07-05	12/06	Hurricane Katrina Activities, Hancock County, Mississippi	$0	$0	$0
6.	DA-07-06	12/06	Hurricane Wilma Activities, City of Coral Gables, Florida	$274,225	$0	$0
7.	DA-07-07	1/07	Hurricane Katrina Activities, Alabama Department of Conservation and Natural Resources	$63,063	$0	$0
8.	DA-07-08	2/07	Hurricane Katrina Activities, Jones County, Mississippi	$0	$0	$0

Appendix 4
Financial Assistance Audit Reports Issued

	Report Number	Date Issued	Auditee	Questioned Costs	Unsupported Costs	Funds Put to Better Use
9.	DD-07-01	10/06	University of Texas Health Science Center, Houston, Texas	$1,427,869	$476,642	$0
10.	DD-07-02	11/06	St. Bernard Parish, Louisiana's Management of Department of Homeland Security Grants Awarded for the Removal of Debris from Hurricane Katrina (Redacted)	$209,115	$0	$0
11.	DD-07-03	12/06	Landfill Cost Issues Relating to Disposal of Debris in the City of New Orleans	$0	$0	$860,000
12.	DD-07-04	1/07	City of Houston, Houston, Texas	$2,052,846	$1,606,658	$0
13.	DD-07-05	2/07	Hurricane Katrina Activities, Plaguemines Parish Sheriff's Office, Louisiana	$1,054,000	$0	$0
14.	DD-07-06	2/07	Contract Costs, Clearbrook, LLC	$16,400,000	$0	$0
15.	DD-07-07	3/07	Hurricane Rita Activities, Jefferson County, Texas	$239,451	$0	$0
16.	DD-07-08	3/07	Hurricane Katrina Activities, City of Kenner, Louisiana	$679,150	$0	$0
			Subtotal, Grant Audits	**$23,046,371**	**$2,083,300**	**$860,000**

Appendix 4
Financial Assistance Audit Reports Issued

	Report Number	Date Issued	Auditee	Questioned Costs	Unsupported Costs	Funds Put to Better Use
---	OIG-07-02	10/06	The State of North Carolina's Management of State Homeland Security Grants Awarded During Fiscal Years 2002 and 2003	$426,578	$123,808	$0
---	OIG-07-06	11/06	Federal Emergency Management Agency's Public Assistance Grant Funds Awarded to the Macon Water Authority After Tropical Storm Alberto	$324,992	$0	$0
---	OIG-07-26	2/07	Federal Emergency Management Agency Public Assistance Grant Funding Awarded to the City of Richmond California After the Loma Prieta Earthquake	$12,169,567	$0	$0
---	OIG-07-31	2/07	Special Transient Accommodations Program for the Evacuees From Hurricanes Katrina and Rita	$3,399,654	$0	$0
			Subtotal (see Notes and Explanations)	**$16,320,791**	**$123,808**	**$0**

Appendix 4
Financial Assistance Audit Reports Issued

	Report Number	Date Issued	Auditee	Questioned Costs	Unsupported Costs	Funds Put to Better Use
17.	OIG-C-01-07	10/06	Report on Audit Proposal for an Energy Savings Performance Contract - Honeywell International, Inc.	$0	$0	$363,150
18.	OIG-C-04-07	10/06	Report on Audit of Incurred Costs for Fiscal Years Ending December 31, 2002 and December 31, 2003 – ICF Consulting Group	$353,701	$353,701	$0
19.	OIG-C-05-07	10/06	Report on Audit of Incurred Costs for Fiscal Year 2003 – Siemens Maintenance Services	$0	$0	$105,924
			Subtotal, DCAA Audits	**$353,701**	**$353,701**	**$469,074**
20.	OIG-S-01-07	10/06	State of New Jersey	$725,810	$543,810	$0
21.	OIG-S-03-07	11/06	Hancock County, Mississippi	$668	$0	$0
22.	OIG-S-07-07	11/06	Guam International Airport Authority	$153,558	$0	$0
23.	OIG-S-09-07	11/06	City of Richmond, CA	$10,712	$0	$0
24.	OIG-S-11-07	11/06	Commonwealth of the Northern Mariana Islands	$713,115	$0	$0
25.	OIG-S-17-07	11/06	United Way of America – Emergency Food and Shelter National Board	$372,395	$360,809	$0
26.	OIG-S-27-07	1/07	American Red Cross National Sector	$1,620,721	$1,619,941	$0
27.	OIG-S-31-07	1/07	City and County of San Francisco CA	$4,296	$4,296	$0

Appendix 4
Financial Assistance Audit Reports Issued

	Report Number	Date Issued	Auditee	Questioned Costs	Unsupported Costs	Funds Put to Better Use
28.	OIG-S-33-07	1/07	City of Fort Madison, IA	$325,000	$325,000	$0
29.	OIG-S-35-07	1/07	City of Albuquerque New Mexico	$998,092	$0	$0
30.	OIG-S-38-07	1/07	City of Indianapolis, IN	$34,964	$34,964	$0
31.	OIG-S-39-07	2/07	City of New York, NY	$299,910	$299,910	$0
32.	OIG-S-56-07	3/07	City of Shreveport, LA	$419,086	$419,086	$0
33.	OIG-S-57-07	3/07	State of Colorado	$7,929,000	$0	$0
			Subtotal, Single Audits	**$13,607,327**	**$3,607,816**	**$0**
			Grand Total Financial Assistance	**$53,328,190**	**$6,168,625**	**$1,329,074**

Notes and Explanations:

The report narratives identify 100 percent of the dollar amount we questioned. However, Appendix 4 reflects the actual breakdown of what the grantee is expected to de-obligate or reimburse to the federal government.

Four management audit reports (OIG-07-02, OIG-07-06, OIG-07-26, and OIG-07-31) are included in Appendix 4 to show the total dollar value of questioned costs disclosed in the reports.

Appendix 4 does not list all Single Audit reports nor all Defense Contract Audit Agency reports we processed, but rather those that disclosed questioned costs or funds put to better use.

Report Number Acronyms:

DA	Disaster, Atlanta Office
DD	Disaster, Dallas Office
OIG-C	Defense Contract Audit Agency report
OIG-S	Single Audit report

Appendix 5
Schedule of Amounts Due and Recovered

	Report Number	Date Issued	Auditee	Amount Due	Recovered Costs
1.	A-S-41-03	07/03	Government of Guam	$0	$182,889
2.	OIG-S-09-07	11/06	City of Richmond, CA	$0	$6,101
			Total	**$0**	**$188,990**

Report Number Acronyms:

A-S Single Audit Report
OIG-S Single Audit report

Appendix 6
Acronyms

ATS	Automated Targeting System
CBP	Customs and Border Protection
CIS	Citizen and Immigration Service
DACS	Deportable Alien control System
DCAA	Defense Contract Audit Agency
DHS	Department of Homeland Security
EMPG	Emergency Management Performance Grant
ePMO	Electronic Program Management Office System
FBI	Federal Bureau of Investigations
FEMA	Federal Emergency Management Directorate
FPS	Federal Protective Service
FY	Fiscal Year
GAO	Government Accountability Office
ICE	Immigration and Customs Enforcement
IPRO	Intelligent Procurement System
IT	Information Technology
NEMIS	National Emergency Management Information System
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PII	Personally Identifiable Information
PEO	Program Executive Office
SAP	Systems Applications Products
SBI	Secure Border Initiative
SBInet	Program to modernize border patrol operations
SIDA	Security Identification Display Area
SPO	Systems Program Office
TSA	Transportation Security Administration
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Services
USDA	United States Department of Agriculture
USSS	United States Secret Service
VITEMA	Virgin Islands Territorial Emergency Management Agency

Appendix 7
OIG Headquarters/Field Office Contacts and Locations

Department of Homeland Security
Attn: Office of Inspector General
245 Murray Drive, SW, Bldg 410
Washington, D.C. 20528

Telephone Number (202) 254-4100
Fax Number (202) 254-4285
Website Address *www.dhs.gov*

OIG Headquarters Senior Management Team

Richard L. Skinner	**……**	**Inspector General**
James L. Taylor	**……**	**Principal Deputy Inspector General**
Matt Jadacki	**……**	**Deputy Inspector General/Office of Disaster Assistance Oversight**
Richard N. Reback	**……**	**Counsel to the Inspector General**
James L. Taylor	**……**	**Acting Assistant Inspector General/Audits**
Elizabeth M. Redman	**……**	**Assistant Inspector General/Investigations**
Carlton I. Mann	**……**	**Assistant Inspector General/Inspections**
Frank Deffer	**……**	**Assistant Inspector General/Information Technology**
Edward F. Cincinnati	**……**	**Assistant Inspector General/Administration**
Tamara Faulkner	**……**	**Congressional Liaison and Media Affairs**
Denise S. Johnson	**……**	**Executive Assistant to the Inspector General**

Appendix 7
OIG Headquarters/Field Office Contacts and Locations
Locations of Audit Field Offices

Boston, MA
Boston, MA 02222
(617) 223-8600 / Fax (617) 223-8651

Chicago, IL
Chicago, IL 60603
(312) 886-6300 / Fax (312) 886-6308

Houston, TX
Houston, TX 77057
(713) 706-4611 / Fax (713) 706-4625

Miami, FL
Miramar, FL 33027
(954) 538-7842 / Fax (954) 602-1034

Philadelphia, PA
Marlton, NJ 08053-1521
(856) 968-4907 / Fax (856) 968-4914

Appendix 7
OIG Headquarters/Field Office Contacts and Locations
Locations of Investigative Field Offices

Atlanta, GA
Atlanta, GA 30309
(404) 832-6730 / Fax (404) 832-6646

Boston, MA
Boston, MA 02222
(617) 565-8705 / Fax (617) 565-8995

Buffalo, NY
Buffalo, NY 14202
(716) 843-5700 x520 / Fax (716) 551-5563

Chicago, IL
Chicago, IL 60603
(312) 886-2800 / Fax (312) 886-2804

Dallas, TX
Denton, TX 76208
(940) 891-8930 / Fax (940) 891-8959

Del Rio, TX
Del Rio, TX 78840
(830) 775-7492 x239

Detroit, MI
Detroit, MI 48226
(313) 226-2163 / Fax (313) 226-6405

El Centro, CA
Imperial, CA 92251
(760) 335-3900 / Fax (760) 335-3726

El Paso, TX
El Paso, TX 79925
(915) 629-1800 / Fax (915) 594-1330

Houston, TX
Houston, TX 77057
(713) 706-4600 / Fax (713) 706-4622

Laredo, TX
Laredo, TX 78045
(956) 796-2917 / Fax (956) 717-0395

Appendix 7
OIG Headquarters/Field Office Contacts and Locations
Locations of Investigative Field Offices

McAllen, TX
McAllen, TX 78501
(956) 664-8010 / Fax (956) 618-8151

Miami, FL
Miramar, FL 33027
(954) 538-7555 / Fax (954) 602-1033

New York City, NY
Jersey City, NJ 07310
(201) 356-1800 / Fax (201) 356-4038

Philadelphia, PA
Marlton, NJ 08053
(856) 596-3800 / Fax (856) 810-3410

San Diego, CA
San Diego, CA 92101
(619) 557-5970 / Fax (619) 557-6518

San Francisco, CA
Oakland, CA 94612
(510) 637-4311 / Fax (510) 637-4327

San Juan, PR
San Juan, PR 00918
(787) 294-2500 / Fax (787) 771-3620

Seattle, WA
Kirkland, WA 98033
(425) 250-1260 / Fax (425) 576-0898

St. Thomas, VI
St. Thomas, VI 00802
(340) 777-1792

Tucson, AZ
Tucson, AZ 85741
(520) 229-6421 / Fax (520) 670-5246

Washington, DC
Arlington, VA 22209
(703) 235-0848 / Fax (703) 235-0854

Yuma, AZ
Yuma, AZ 85365
(928) 314-9640

Appendix 7
OIG Headquarters/Field Office Contacts and Locations
Locations of DAO Field Offices

Atlanta, GA
Atlanta, GA 30309
(404) 832-6700 / Fax (404) 832-6645

Austin, TX
Austin, TX 78753
(512) 908-8700 / Fax (512) 977-4640

Baton Rouge, LA
Baton Rouge, LA 70802
(225) 242-6000 / Fax (225) 379-4020

Biloxi, MS
Biloxi, MS
(220) 385-5605

Dallas, TX
Denton, TX 76208
(940) 891-8900 / Fax (940) 891-8948

Jackson, MS
Jackson, MS 39201
(601) 965-2599 / Fax (601) 965-2432

Montgomery, AL
Montgomery, Al 36117
(334) 409-4634

New Orleans, LA
New Orleans, LA 70114
(504) 762-2151 / Fax (504) 762-2873

Orlando, FL
Orlando, FL 32809
(407) 856-3204

San Francisco, CA
Oakland, CA 94612
(510) 637-4311 / Fax (510) 637-1484

San Juan, PR
San Juan, PR 00918
(787) 294-2500 / Fax (787) 771-3620

Appendix 8
Index to Reporting Requirements

The specific reporting requirements described in the *Inspector General Act of 1978*, as amended, are listed below with a reference to the SAR pages on which they are addressed.

Requirement:	**Pages**
Review of Legislation and Regulations	55
Significant Problems, Abuses, and Deficiencies	6-51
Recommendations with Significant Problems	6-51
Prior Recommendations Not Yet Implemented	53-54
Matters Referred to Prosecutive Authorities	2
Summary of Instances Where Information Was Refused	N/A
List of Audit Reports	84-91
Summary of Significant Audits	6-51
Reports with Questioned Costs	80
Reports Recommending That Funds Be Put To Better Use	82
Summary of Reports in Which No Management Decision Was Made	80-82
Revised Management Decisions	N/A
Management Decision Disagreements	N/A

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, 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 e-mail DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer.