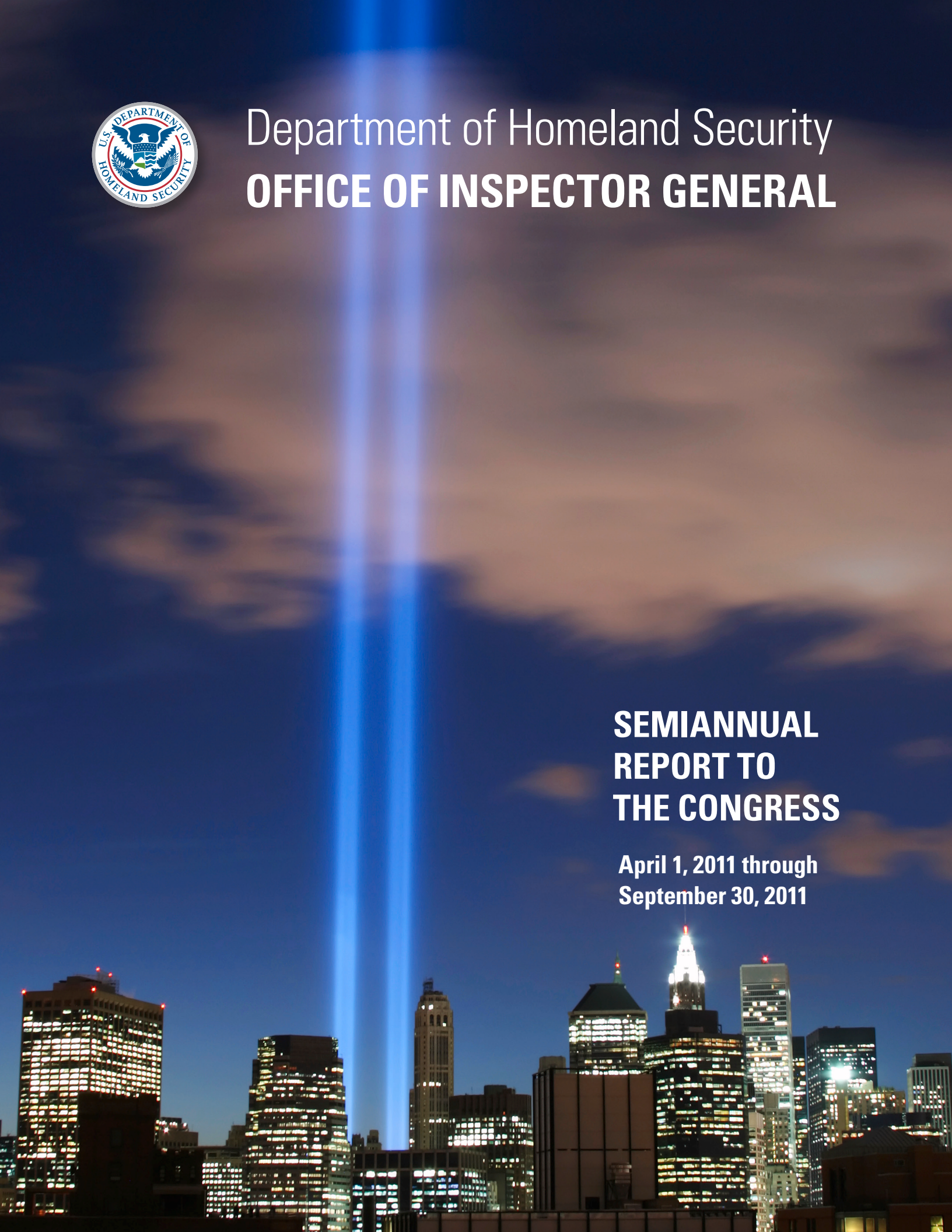


Department of Homeland Security

OFFICE OF INSPECTOR GENERAL

SEMIANNUAL REPORT TO THE CONGRESS

April 1, 2011 through
September 30, 2011

Statistical Highlights of OIG Activities

April 1, 2011 through September 30, 2011

Dollar Impact	
Questioned Costs	$855,383,832
Funds Put to Better Use	$10,302,337
Management Agreement That Funds Be:	
Recovered	$676,749,966
Deobligated	$4,372,843
Funds Recovered (from audits and investigations)	$19,857,504
Fines, Restitutions, and Administrative Cost Savings	$20,458,388

Activities	
Management Reports Issued	51
Financial Assistance Grant Audit Reports	31
Council of the Inspectors General on Integrity and Efficiency Reports Issued	3
Investigative Reports Issued	391
Investigations Initiated	715
Investigations Closed	433
Open Investigations	2,564
Investigations Referred for Prosecution	202
Investigations Accepted for Prosecution	81
Investigations Declined for Prosecution	74
Arrests	154
Indictments	110
Convictions	136
Personnel Actions	65
Total Complaints Received	11,017
Complaints Referred (to programs or other agencies)	7,815
Complaints Closed	8,933

Office of Inspector General

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

Homeland Security

October 31, 2011

The Honorable Janet Napolitano
Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Dear Madam 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 (OIG) for the 6-month period ended September 30, 2011.

During this reporting period, our office published 51 management reports and 31 financial assistance grant reports. DHS management concurred with 93% of recommendations contained in our management reports. As a result of these efforts, $855.4 million of questioned costs were identified, of which $62.3 million were determined to be unsupported by documentation. We recovered $19.9 million as a result of disallowed costs identified from previous audit reports and from investigative efforts. We issued 12 reports identifying $10.3 million in funds that could be put to better use. In addition, management agreed to deobligate $4.4 million in disaster grant assistance, which will result in funds put to better use.

In the investigative area, we issued 391 investigative reports, initiated 715 investigations, and closed 433 investigations. Our investigations resulted in 154 arrests, 110 indictments, 136 convictions, and 65 personnel actions. Additionally, we reported $20.5 million in collections resulting from fines and restitutions, administrative cost savings, and other recoveries.

I would like to take this opportunity to thank you for the interest and support that you have provided to our office. We look forward to working closely with you, your leadership team, and Congress to promote economy, efficiency, and effectiveness in DHS programs and operations, and to help the Department accomplish its critical mission and initiatives in the months ahead.

Sincerely,

Charles K. Edwards
Acting Inspector General

U.S. DEPARTMENT OF HOMELAND SECURITY

Table of Contents

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 together most effectively, 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 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 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. The agency should allow the OIG timely access to agency records and other materials.

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 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 will keep agency management 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 will implement mechanisms, both formal and informal, to ensure prompt and regular feedback.

Executive Summary

This Semiannual Report to the Congress is issued pursuant to the provisions of Section 5 of the *Inspector General Act of 1978*, as amended, and covers the period from April 1, 2011 to September 30, 2011. The report is organized to reflect our organization and that of the Department of Homeland Security.

During this reporting period, we completed significant audit, inspection, and investigative work to promote the economy, efficiency, effectiveness, and integrity of the Department's programs and operations. Specifically, we issued 51 management reports (appendix 3), 31 financial assistance grant reports (appendix 4), and 391 investigative reports. Our reports provide the Department Secretary and Congress with an objective assessment of the issues, and at the same time provide specific recommendations to correct deficiencies and improve the economy, efficiency, and effectiveness of the respective program.

Also, our audits resulted in questioned costs of $855,383,832, of which $62,263,057 was not supported by documentation. We recovered $19,857,504 (appendix 5) as a result of disallowed costs identified from current and previous audit reports and from investigative efforts. We issued 12 reports identifying $10,302,337 in funds that could be put to better use. In addition, management agreed to deobligate $4,372,843 in disaster grant assistance, which will result in funds put to better use. In the investigative area, we initiated 715 investigations and closed 433 investigations. Our investigations resulted in 154 arrests, 110 indictments, 136 convictions, and 65 personnel actions. Additionally, we reported $20,458,388 in collections resulting from fines and restitutions, administrative cost savings, and other recoveries.

We have a dual reporting responsibility to both the Congress and the Department Secretary. During the reporting period, we continued our active engagement with Congress through extensive meetings, briefings, and dialogues. Members of Congress, their staffs, and the Department's authorizing and appropriations committees and subcommittees met on a range of issues relating to our work and that of the Department. We also testified before Congress on two occasions during this reporting period. Testimony prepared for these hearings may be accessed through our website at **www.oig.dhs.gov/**.

Department of Homeland Security Profile

On November 25, 2002, President Bush signed the *Homeland Security Act of 2002* (P.L. 107-296, as amended), officially establishing DHS, with the primary mission of protecting the American homeland. DHS became operational on January 24, 2003. 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 United States (U.S.) 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 is organized into the following major components:

- Directorate for Management
- Directorate for National Protection and Programs
- Directorate for Science and Technology
- Domestic Nuclear Detection Office
- Federal Emergency Management Agency
- Federal Law Enforcement Training Center
- Office for Civil Rights and Civil Liberties
- Office of General Counsel
- Office of Health Affairs
- Office of Inspector General
- Office of Intelligence and Analysis
- Office of Operations Coordination and Planning
- Office of Policy
- Privacy Office
- 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

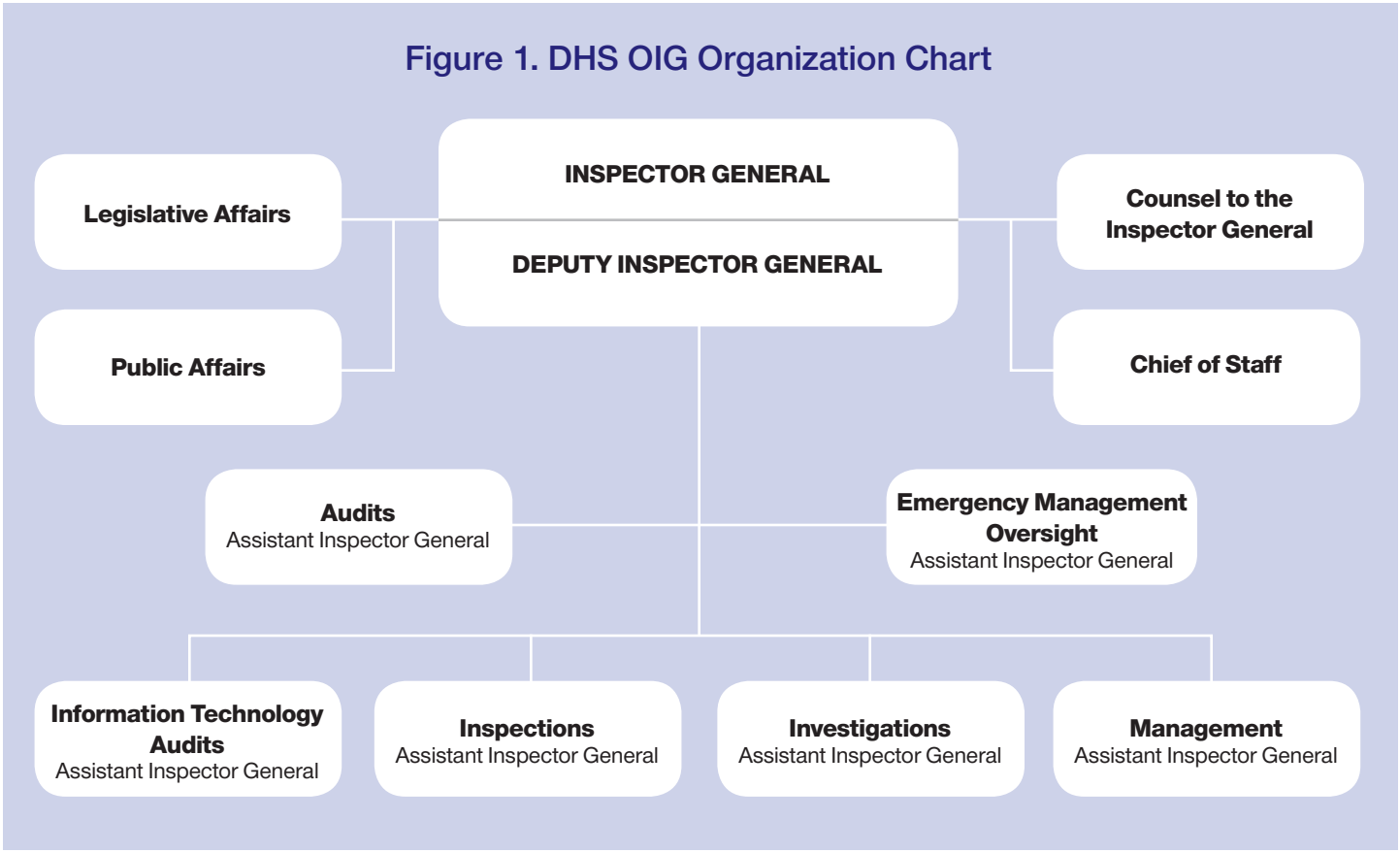
Office of Inspector General Profile

The *Homeland Security Act of 2002* provided for the establishment of an 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 were authorized 676 full-time employees during the reporting period. We consist of an Executive Office and ten functional components based in Washington, DC. We also have field offices throughout the country. Figure 1 illustrates the DHS OIG management team.

Figure 1. DHS OIG Organization Chart



DHS OIG consists of the following components:

The Executive Office consists of the Inspector General, the Deputy Inspector General, a Chief of Staff, a Senior Management Analyst, and a Special Assistant. It provides executive leadership to the OIG.

The Office of Legislative Affairs (OLA) is the primary liaison to members of Congress and their staffs. Specifically, OLA's staff responds to inquiries from Congress; notifies Congress about OIG initiatives, policies, and programs; coordinates preparation of testimony and talking points for Congress; and coordinates distribution of reports and correspondence to Congress. Office staff tracks congressional requests, which are either submitted by a member of Congress or mandated through legislation. OLA also provides advice to the Inspector General and supports OIG staff as they address questions and requests from Congress.

The Office of Public Affairs (OPA) is the Inspector General's principal point of contact for the media and the public. OPA provides information about OIG and its audit, inspection, and investigative reports and recommendations to news organizations and the public in compliance with legal, regulatory, and procedural rules. OPA prepares and issues news releases, arranges interviews, and coordinates and analyzes information to support OIG's policy development and mass communications needs. OPA is also responsible for crisis communication management, social media engagement, and employee communication. OPA advises the Inspector General and others within the OIG by analyzing trends, predicting their consequences, counseling OIG senior staff, and implementing planned programs of action, which serve both the organization and the public interest.

The Office of Counsel to the Inspector General (OC) provides legal advice to the Inspector General and other management officials; supports audits, inspections, and investigations by ensuring that applicable laws and regulations are followed; serves as the OIG's designated ethics office; manages the OIG's *Freedom of Information Act* (FOIA) and *Privacy Act* responsibilities; furnishes attorney services for the issuance and enforcement of OIG subpoenas; and provides legal advice on OIG operations.

The Office of Audits (OA) conducts and coordinates audits and program evaluations of the management and financial operations of DHS. Auditors examine the methods that agencies, bureaus, grantees, and contractors employ in carrying out essential programs or activities. Audits evaluate whether established goals and objectives are achieved, resources are used economically and efficiently, and intended and realized results are consistent with laws, regulations, and good business practice; and determine whether financial accountability is achieved and the financial statements are not materially misstated.

The Office of Emergency Management Oversight (EMO) provides an aggressive and ongoing audit effort designed to ensure that disaster relief funds are spent appropriately, while identifying fraud, waste, and abuse as early as possible. EMO keeps the Congress, the Secretary, the Administrator

of the Federal Emergency Management Agency (FEMA), and others fully informed on problems relating to disaster operations and assistance programs, and progress regarding corrective actions. EMO's focus is weighted heavily toward prevention, including reviewing internal controls, and monitoring and advising DHS and FEMA officials on contracts, grants, and purchase transactions before they are approved. This allows EMO to stay current on all disaster relief operations and provide on-the-spot advice on internal controls and precedent-setting decisions. A portion of its full-time and temporary employees are dedicated to Gulf Coast hurricane recovery.

The Office of Information Technology Audits (ITA) conducts audits and evaluations of DHS' information management, cyber infrastructure, and systems integration activities. ITA reviews the cost-effectiveness of acquisitions, implementation, and management of major systems and telecommunications networks across DHS. In addition, it evaluates the systems and related architectures of DHS to ensure that they are effective, efficient, and implemented according to applicable policies, standards, and procedures. ITA also assesses DHS' information security program as mandated by the *Federal Information Security Management Act*. In addition, ITA provides technical forensics assistance to OIG offices in support of OIG's fraud prevention and detection program.

The Office of Inspections (ISP) provides the Inspector General with a means to analyze programs quickly and to evaluate operational efficiency, effectiveness, and vulnerability. This work includes special reviews of sensitive issues that arise suddenly and congressional requests for studies that require immediate attention. ISP may examine any area of the Department. In addition, it is the lead OIG office for reporting on DHS intelligence, international affairs, civil rights and civil liberties, and science and technology. Inspectors use a variety of study methods and evaluation techniques to develop recommendations for DHS. Inspection reports are released to DHS, Congress, and the public.

The Office of Investigations (INV) investigates allegations of criminal, civil, and administrative misconduct involving DHS employees, contractors, grantees, and programs. These investigations can result in criminal prosecutions, fines, civil monetary penalties, administrative sanctions, and personnel actions. Additionally, INV provides oversight and monitors the investigative activity of DHS' various internal affairs offices. INV includes investigative staff working on Gulf Coast hurricane recovery operations.

The Office of Management (OM) provides critical administrative support functions, including OIG strategic planning; development and implementation of administrative directives; the OIG's information and office automation systems; budget formulation and execution; correspondence; printing and distribution of OIG reports; and oversight of the personnel, procurement, travel, and accounting services provided to the OIG on a reimbursable basis by the Bureau of Public Debt. OM also prepares the OIG's annual performance plan and semiannual reports to Congress.

SUMMARY OF SIGNIFICANT OFFICE OF INSPECTOR GENERAL (OIG) ACTIVITY

DIRECTORATE FOR MANAGEMENT

MANAGEMENT REPORTS

DHS Oversight of Component Acquisition Programs

The DHS revised enacted budget authority for fiscal year (FY) 2010 is approximately $55.3 billion. Between October 2009 and August 2010, DHS obligated approximately $9.2 billion in procurement costs. Based on our review of 17 acquisition programs, with a cost estimate of $9.6 billion, the Department needs to refine its revised acquisition management directive by providing additional detailed guidance and improve controls over acquisition programs. Some components inappropriately created program management offices to manage simple procurements, did not properly report programs into the standard system, or did not apply strategic sourcing strategies to support program development. Additionally, not all components developed component-level acquisition policies and procedures to manage programs at the component level. As a result, the Department does not know what is in its acquisition portfolio, and components unnecessarily created acquisition program management offices, which potentially increased administrative costs without adding value to the programs.

We made four recommendations to the Department's Chief Procurement Officer to strengthen its management oversight and controls over component acquisition programs, which it agreed with and, during the audit, initiated action to correct. When fully implemented, these actions should help enhance the effectiveness of the Department's acquisition management process.
(OIG-11-71, April 2011, OA)
http://www.oig.dhs.gov/assets%5CMgmt%5COIG_11-71_Apr11.pdf

Update on DHS' Procurement and Program Management Operations

We conducted a follow-up review to determine the progress the Department has made implementing prior recommendations from our 2005 DHS's procurement and program management operations. As a result, we reported that the Department has implemented all five of the prior report's recommendations by addressing staffing issues and developing important oversight policies and guidance. These actions have improved and standardized DHS' procurement and program management operations. During our review, we identified two additional areas for suggested improvement in the areas of ethics training and reporting.
(OIG-11-91, June 2011, OA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-91_Jun11.pdf

Use of DHS Purchase Cards

In FY 2009, DHS made about 1.2 million purchases valued at about $520 million for goods and services using purchase cards. Although purchase card use does reduce administrative procurement costs, control weaknesses can increase the risk of inappropriate purchase card use. We performed this audit to determine whether DHS has internal controls in place to ensure that purchase cards are used for their intended purpose. The Department generally had an effective internal control framework developed. However, the Department needs to improve specific internal control procedures to mitigate the inherent risks associated with purchase card use. The Department's post payment audit process did not ensure that component personnel were meeting minimum internal control requirements established by the Office of Management and Budget (OMB). Nor did the process effectively target high-risk transactions for review. Also, the Department's purchase card manual and components' guidance were incomplete or inconsistent. The Office of the Chief Financial Officer concurred with our three recommendations, and has already initiated some corrective actions based on our audit.
(OIG-11-101, August 2011, OA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-101_Aug11.pdf

Information Technology Management Letter for the FY 2010 DHS Financial Statement Audit
KPMG LLP, under contract with DHS OIG, performed a review of DHS information technology (IT) general controls in support of the FY 2010 DHS financial statement engagement. The overall objective of this review was to evaluate the effectiveness of IT general controls of DHS' financial processing environment and related IT infrastructure as necessary to support the engagement. KPMG LLP also performed technical security testing for key network and system devices, as well as testing over key financial application controls. KPMG LLP noted that DHS took corrective action to address many prior years' IT control weaknesses. However, during FY 2010, KPMG continued to find IT general control weaknesses at each component. The most significant weaknesses from a financial statement audit perspective related to entity-wide security, access controls, and service continuity. Collectively, the IT control weaknesses limit DHS' ability to ensure that critical financial and operational data are maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively impact the internal controls over DHS' financial reporting and its operation, and KPMG LLP considers them to collectively represent a material weakness under standards established by the American Institute of Certified Public Accountants (AICPA). (OIG-11-103, August 2011, ITA)
http://www.oig.dhs.gov/assets/Mgmt/OIGr_11-103_Aug11.pdf

Evaluation of DHS' Information Security Program for Fiscal Year 2011
DHS has continued to take steps to improve and strengthen its information security program. While these efforts have resulted in some improvements, components are still not executing all of the Department's policies, procedures, and practices. For example, our review identified several exceptions to a strong and effective information security program: (1) systems are being authorized though key information is missing or outdated; (2) plans of action and milestones (POA&M) are not being created for all known information security weaknesses or mitigated in a timely manner; and (3) baseline security configurations are not being implemented for all systems. Additional information security program areas that need improvement include incident detection and analysis, specialized training, account and identity management, continuous monitoring, and contingency planning.

We made five recommendations aimed at improving DHS' information security program, including improvements in continuous monitoring, POA&M, security authorization, and DHS baseline configuration areas. The Department concurred with all five recommendations. (OIG-11-113, September 2011, ITA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-113_Sep11.pdf

DHS Continues To Face Challenges in the Implementation of Its OneNet Project
DHS began to consolidate and transform its existing individual component networks into a single world-class information technology infrastructure. To achieve this goal, the OneNet Infrastructure, an enterprise-wide integrated information technology network, was created. The goal of OneNet is to create a reliable, cost-effective information technology infrastructure platform that supports the ability to share data among components. We reviewed the Department's efforts to consolidate component networks to OneNet. Our objective was to determine the progress the Department is making in meeting its OneNet objectives. Generally, the Department has made some progress toward consolidating the existing components' infrastructures into OneNet. Specifically, it has established a centralized Network Operations Center/Security Operations Center incident response center. Further, components are signing Memorandums of Agreement and converting their sites to the Multiple Protocol Label Switching architecture in accordance with OneNet requirements. Finally, the Department has established the redundant trusted Internet connection that provides a redundant network infrastructure and offers essential network services to its components.

However, the Department needs to make a number of improvements in order to successfully implement the OneNet architecture. Specifically, it needs to establish component connections (peering) to OneNet and ensure that all components transition to the redundant trusted internet connection. Further, it needs to complete required project management documents, and update interconnection security agreements. (OIG-11-116, September 2011, ITA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-116_Sep11.pdf

DIRECTORATE FOR NATIONAL PROTECTION AND PROGRAMS

MANAGEMENT REPORTS

Planning, Management, and Systems Issues Hinder DHS' Efforts To Protect Cyberspace and the Nation's Cyber Infrastructure
Cybersecurity risks pose some of the most serious economic and national security challenges our Nation faces. DHS is the principal focal point for the security of cyberspace and the national effort to protect critical infrastructure and key resources. This report identifies measures the National Protection and Programs Directorate (NPPD) can take to enhance the overall effectiveness of the Department's efforts to secure cyberspace and the Nation's cyber infrastructure. While DHS has made progress in sharing cybersecurity threat information, raising cybersecurity awareness, and implementing educational programs that focus on cybersecurity, significant work remains to address the open actions and recommendations and attain the goals outlined in *The National Strategy to Secure Cyberspace*, National Infrastructure Protection Plan, and Comprehensive National Cybersecurity Initiative. We made ten recommendations that focus on robust strategic planning and developing performance measures needed to reduce risks and threats; ensuring that systems personnel receive required Protected Critical Infrastructure Information training; and mitigating configuration and account access vulnerabilities to ensure the confidentiality, integrity, and availability of the Department's critical infrastructure and asset data and the systems used to capture, store, and protect that information. NPPD management concurred with the recommendations and has already begun to take actions to implement them.
(OIG-11-89, June 2011, ITA)
http://www.oig.dhs.gov/assets/Mgmt/OIGr_11-89_Jun11.pdf

DHS Risk Assessment Efforts in the Dams Sector
A primary mission of DHS is to protect the Nation's 18 critical infrastructure sectors, one of which is the Dams Sector, against terrorist attacks and other natural and manmade hazards. The Dams Sector consists of dams, navigation locks, levees, and other similar water retention and control facilities, collectively known as "dam assets." These critical dam assets are owned by private entities, federal agencies, and state and local governments.

Because the Department works mainly within a largely voluntary partnership framework, it lacks assurance that risk assessments were conducted and security risks associated with critical dams were identified and mitigated. Underlying legislation does not give the Department the necessary authority to ensure that security partners participate in risk management activities, or that dam owners undergo Departmental assessments and implement corrective action.

The Department could not always obtain cooperation from its security partners, and dam owners and did not always collaborate successfully. We recommended that the Assistant Secretary, Office of Infrastructure Protection, determine the appropriateness of a legislative proposal to establish regulatory authority for the critical Dams Sector assets similar to the Chemical Sector.
(OIG-11-110, September 2011, OA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-110_Sep11.pdf

FEDERAL EMERGENCY MANAGEMENT AGENCY

MANAGEMENT REPORTS

Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology

FEMA is responsible for developing federal response capability to deliver assistance in a natural or manmade disaster or act of terrorism. Historically, FEMA's IT systems have not fully supported the agency's needs during major disasters. In this review, we concluded that FEMA's existing IT systems still do not support disaster response activities effectively. Specifically, the agency has a number of IT infrastructure modernization initiatives underway; however, it does not have a comprehensive IT strategic plan or enterprise architecture to provide guidance needed. In addition, the Office of the Chief Information Officer (CIO) does not have a documented inventory of its systems to support disasters. Finally, the office has completed improvements to its infrastructure foundation; however, efforts to modernize some of the agency's critical IT systems have been put on hold due to departmental consolidation plans. We recommended that the CIO develop a comprehensive IT strategic plan; complete and implement a FEMA enterprise architecture; establish an enterprise IT systems inventory; establish an agency-wide IT budget planning process; obtain agency-wide IT investment review authority; and establish a consolidated modernization approach for FEMA's mission-critical IT systems.
(OIG-11-69, April 2011, ITA)
http://www.oig.dhs.gov/assets%5CMgmt%5COIG_11-69_Apr11.pdf

Federal Emergency Management Agency's Management Letter for FY 2010 DHS Consolidated Financial Statements Audit

KPMG LLP, under contract with DHS OIG, reviewed FEMA's internal control over financial reporting. The management letter discusses 16 observations for management's consideration identified during the FY 2010 financial statement audit. These observations were discussed with the appropriate members of management and are intended to improve internal control or result in other operating efficiencies. These issues did not meet the criteria to be reported in the *Independent Auditors' Report on DHS' FY 2010 Financial Statements and Internal Control over Financial Reporting*, dated November 12, 2010, included in the *Department of Homeland Security FY 2010 Annual Financial Report*.
(OIG-11-75, April 2011, OA)
http://www.oig.dhs.gov/assets%5CMgmt%5COIG_11-75_Apr11.pdf

Opportunities to Improve FEMA's Mass Care and Emergency Assistance Activities

The Mass Care and Emergency Assistance program is the primary component of the National Response Framework's Emergency Support Function 6. The Mass Care and Emergency Assistance program assists state, local, and tribal governments and private non-profit organizations in the coordination of disaster assistance in the aftermath of a disaster. To improve FEMA effectiveness in managing and coordinating mass care and emergency assistance, FEMA needs to finalize standard operating procedures, evaluate the effectiveness of the tools and initiatives that have been developed, and ensure that mass care and emergency assistance activities are tested during exercises. Additional action is needed to link the FEMA and American Red Cross National Shelter System databases. This report addresses each of these areas and makes recommendations for improvements.
(OIG-11-77, April 2011, EMO)
http://www.oig.dhs.gov/assets%5CMgmt%5COIG_11-77_Apr11.pdf

Design and Implementation of the Federal Emergency Management Agency's Emergency Management Performance Grant

We reviewed the Emergency Management Performance Grant (EMPG) program to determine if the program's design, implementation, and performance measurement strategy facilitate improved emergency management and preparedness for the grantees. The EMPG program is designed to facilitate emergency management and preparedness. However, FEMA can improve implementation of the program by awarding

grant funds in a timelier manner. Additionally, FEMA has developed, but not yet finalized or implemented, a strategy to measure the effectiveness of program funds.

The report contains two recommendations to FEMA that, when implemented, will enhance the EMPG's overall effectiveness. FEMA concurred with one recommendation and the intent of the other recommendation, and outlined plans and actions to help strengthen the execution and measurement of the program.
(OIG-11-78, April 2011, OA)
http://www.oig.dhs.gov/assets%5CMgmt%5COIG_11-78_Apr11.pdf

Information Technology Management Letter for the Federal Emergency Management Agency Component of the FY 2010 DHS Financial Statement Audit
KPMG LLP, under contract with DHS OIG, performed the audit of the FEMA Consolidated Balance Sheet and related statements as of September 30, 2010. As part of this review, KPMG LLP noted certain matters involving internal control and other operational matters with respect to IT and documented its comments and recommendation in the IT Management Letter. The overall objective of our audit was to evaluate the effectiveness of IT general controls of FEMA's financial processing environment and related IT infrastructure. KPMG LLP noted that FEMA took corrective action to address many prior years' IT control weaknesses. However, during FY 2010, KPMG LLP continued to find IT general control weaknesses at FEMA. The most significant weaknesses from a financial statement audit perspective related to access controls, change control, entity-wide security, system software, and service continuity. Collectively, the IT control weaknesses limit FEMA's ability to ensure that critical financial and operational data are maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively impact the internal controls over FEMA's financial reporting and its operation, and KPMG considers them to collectively represent a material weakness under standards established by AICPA.
(OIG-11-79, May 2011, ITA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-79_May11.pdf

The State of Nevada's Management of State Homeland Security Program and Urban Areas Security Initiative Grants Awarded During Fiscal Years 2006 through 2008
The State of Nevada received approximately $23.1 million in State Homeland Security Program grants and $26.1 million in Urban Areas Security Initiative grants awarded by FEMA during fiscal years 2006 through 2008. Foxx & Company, under a contract with DHS OIG, conducted an audit of these grants to determine whether the state spent funds strategically, effectively, and in compliance with laws, regulations, and guidance.

Generally, the State Administrative Agency did an efficient job of administering the program and distributing grant funds. The state's plans linked funding to all-hazard capabilities and to goals that were established based on risk assessments. Also, the state established an effective system for identifying vulnerabilities and opportunities to improve its preparedness and response capabilities. Grants were generally administered in compliance with applicable laws, regulations, and guidance.

However, improvements were needed in the state's management of the State Homeland Security Program grants regarding its establishment of measurable goals and objectives, identification of long-term capability sustainment options, and monitoring of subgrantee activities. Our six recommendations call for FEMA to require the State of Nevada to initiate improvements that, if implemented, should help strengthen program management, performance, and oversight.
(OIG-11-83, May 2011, OA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-83_May11.pdf

Assessment of FEMA's Fraud Prevention Efforts
Since hurricanes Katrina and Rita, FEMA has disbursed more than $7 billion in Individuals and Households Program disaster assistance program payments. The susceptibility of this program to fraud, waste, and abuse requires increased vigilance on the agency's part in order to be a better steward of taxpayer money. The agency's Fraud Prevention and Investigation Branch (FPIB) has succeeded in identifying and reporting potential fraud to our Office of Investigations, but is hampered by a limited mandate, inadequate staffing, and outdated IT. FEMA's leaders must do more to demonstrate fiscal responsibility and program integrity. Internal controls have improved, but we, the Government Accountability Office (GAO), and FEMA continue to identify needed actions.

The Riverview section of Fargo is experiencing flooding.
Source: FEMA Photo Library

Planning meeting with FEMA personnel.
Source: FEMA Photo library

We made eight recommendations, that, when implemented, will improve fraud prevention efforts. These recommendations include: (1) an agency-wide mandate to review claims of fraud, waste, and abuse, additional staffing, and fraud prevention tools for the FPIB; (2) annual fraud prevention training for all FEMA employees; (3) continual improvement of internal controls; and (4) resolution of the 167,000 cases ($643 million) of potential improper payments disbursed since Hurricane Katrina, which FEMA began to collect in March 2011.
(OIG-11-84, May 2011, EMO)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-84_May11.pdf

Effectiveness and Costs of FEMA's Disaster Housing Assistance Program
The Disaster Housing Assistance Program (DHAP) provided disaster housing assistance to survivors from hurricanes Katrina, Rita, Gustav, and Ike through two separate interagency agreements with the Department of Housing and Urban Development (HUD). Although DHAP for Katrina cost more than $550 million and housed close to 37,000 disaster households and DHAP Ike cost more than $281 million and housed more than 25,000 disaster households, there were neither adequate self-sufficiency nor cost-effectiveness data to evaluate these programs. FEMA needs to conduct a cost-benefit analysis for the Karina and Ike DHAPs to determine if they were cost competitive with other housing options such as FEMA's own Individual and Households Rental Program. FEMA needs to better manage any future DHAP interagency agreements with HUD by establishing requirements for additional cost and program effectiveness data. In addition, FEMA should evaluate administrative and case management fees and, if appropriate, should consider cost reductions for any future DHAPs. This report addresses each of these areas and contains two recommendations for improvements.
(OIG-11-102, August 2011, EMO)
http://www.oig.dhs.gov/assets/mgmt/OIG_11-102_Aug11.pdf

FEMA's Contracting Officer's Technical Representatives Program

FEMA relies on contractors to supplement much of its mission. FEMA's contracting officer's technical representatives (COTRs) play a vital role in verifying that FEMA receives from its contractors the contracted goods and services. As we learned from Hurricane Katrina, when COTRs do not perform their duties, millions of dollars can be wasted. Since Hurricane Katrina, FEMA has dedicated resources to developing its COTR program. We concluded that FEMA has improved its COTR program; however, there is more work to be done. FEMA's improvements include (1) a much larger COTR cadre, with more than 1,400 trained COTRs, (2) a FEMA intranet site dedicated to the COTRs, with guidance, policies, and forms for their use, and (3) FEMA's Office of Chief Procurement Officer has staff dedicated to administering its program. We looked more closely at FEMA's COTR program, its policies and practices, as well as disaster staffing. FEMA has developed COTR specific policies, but COTRs are not always taking advantage of the available policies. FEMA requires its COTRs to be trained, but the COTRs do not believe the training is sufficient for their success. While FEMA has a large number of trained COTRs, there is no plan as to how they will be deployed during a disaster. And although FEMA hires disaster-specific employees, they have not taken advantage of policies made available by the Office of Personnel Management to obtain the best qualified employees to administer contracts. Our report contains eight recommendations that we believe, when implemented, will improve FEMA's COTR cadre.
(OIG-11-106, September 2011, EMO)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-106_Sep11.pdf

The Commonwealth of Pennsylvania's Management of State Homeland Security Program and Urban Areas Security Initiative Grants Awarded During Fiscal Years 2007 through 2009

The Commonwealth of Pennsylvania received $79 million in State Homeland Security Program grants and $75 million in Urban Areas Security Initiative grants awarded by FEMA during fiscal years 2007 through 2009. This audit was mandated by Public Law 110-53, *Implementing Recommendations of the 9/11 Commission Act of 2007,* to determine (1) whether grant funds were distributed and spent effectively, efficiently, and in compliance with applicable federal laws and regulations, and (2) the extent to which the commonwealth has measured improvements in its ability to prevent, prepare for, protect against, and respond to disasters and acts of terrorism.

Generally, the State Administrative Agency administered grant program requirements effectively and efficiently and in compliance with grant guidance and regulations. Program goals and objectives were linked to national priorities and DHS mission areas, grant funds were spent on allowable items and activities, and adequate controls existed over the approval of expenditures and reimbursement of funds.

However, improvements were needed in Pennsylvania's management of the grants in the areas of prioritization of strategic goals and project proposals, development of measurable goals and objectives, obligation of grant funds to subgrantees, and implementation of subgrantee monitoring procedures. Our five recommendations call for FEMA to require the Commonwealth of Pennsylvania to initiate improvements, which, if implemented, should help strengthen grant program management, performance, and oversight. FEMA concurred with all of the recommendations.
(OIG-11-109, September 2011, OA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-109_Sep11.pdf

The State of New Jersey's Management of State Homeland Security Program and Urban Areas Security Initiative Grants Awarded During Fiscal Years 2007 through 2009

The State of New Jersey received $67 million in State Homeland Security Program grants and $106 million in Urban Areas Security Initiative grants awarded by FEMA during fiscal years 2007 through 2009. This audit was mandated by Public Law 110-53, *Implementing Recommendations of the 9/11 Commission Act of 2007*, to determine (1) whether grant funds were distributed and spent effectively, efficiently, and in compliance with applicable federal laws and regulations, and (2) the extent to which the state has measured improvements in its ability to prevent, prepare for, protect against, and respond to disasters and acts of terrorism.

Generally, the State of New Jersey distributed and spent State Homeland Security Program and Urban Areas Security Initiative grant funds effectively and efficiently and in compliance with applicable federal laws and regulations. The state effectively developed its Homeland Security Strategic Plan, and allocated and spent funds based on national and state priorities.

However, improvements were needed in New Jersey's management of the grants in the areas of performance measurement, onsite monitoring, timely obligation and expenditure of grant funds, and federal inventory and accountability requirements. We also questioned $2,657,212 of unallowable or undocumented costs, and identified $585,519 in funds that could be put to better use. Our 11 recommendations call for FEMA to require the State of New Jersey to initiate improvements, which, if implemented, should help strengthen grant program management, performance, and oversight. FEMA concurred with all of the recommendations. (OIG-11-112, September 2011, OA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-112_Sep11.pdf

Improving FEMA's Individual Assistance, Technical Assistance Contracts

The FEMA Individual Assistance, Technical Assistance Contracts (IA-TACs) are for comprehensive program management services as well as construction, architectural, and engineering capabilities to support housing; mass care; and disaster planning, staffing, and logistics services. Each contractor must be capable of supporting multiple disaster missions, anywhere within the United States and its territories. We concluded that there is no guarantee that the contractors will be able to perform when needed. As a result, FEMA is spending, on average, more than $5.1 million each year on readiness capabilities that may not be available when needed.

In addition, FEMA needs to improve its acquisition function. Although the agency has attempted to improve contract management, there is still a need for substantial improvement. Improvements in contract file documentation and better management oversight, including the prompt implementation of corrective actions, are needed to prevent opportunities for fraud, waste, and abuse.

We recommended that FEMA's Director, Individual Assistance Division, coordinate with the Chief Procurement Officer to replace, as soon as practicable, the IA-TACs; ensure that future contracts include specific performance requirements and deliverables; and ensure that acquisition personnel assigned to manage and monitor contracts have the requisite skills and abilities. (OIG-11-114, September 2011, EMO)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-114_Sep11.pdf

DISASTER ASSISTANCE GRANTS

The Robert T. Stafford Disaster Relief and Emergency Assistance Act (P.L. 93-288), as amended, governs disasters declared by the President of the United States. Title 44 of the Code of Federal Regulations provides further guidance and requirements for administering disaster assistance grants awarded by FEMA. We review grants to ensure that grantees or subgrantees account for and expend FEMA funds according to federal regulations and FEMA guidelines.

We issued 31 financial assistance grant reports during the period. Those reports disclosed questioned costs totaling $209,423,146, of which $61,098,539 was unsupported. A list of these reports, including questioned costs and unsupported costs, is provided in appendix 4.

Mississippi State Port Authority
The Mississippi State Port Authority (MSPA) received a public assistance award of $72.9 million from the Mississippi Emergency Management Agency (MEMA), a FEMA grantee, for damages related to Hurricane Katrina, which occurred in August 2005. The award provided 100% FEMA funding for debris removal, emergency protective measures, and permanent repairs to damaged facilities. Our audit focused primarily on $32.9 million claimed under five large projects. MSPA accounted for large project expenditures on a project-by-project basis as required by federal regulations. However, MSPA did not always comply with FEMA guidelines when contracting for debris removal work. We questioned $3.2 million of unsupported and ineligible debris removal costs, and determined that $1.3 million of project funding should be deobligated and put to better use. We also determined that MEMA did not properly account for costs related to MSPA's alternate projects. We recommended that the Regional Administrator, FEMA Region IV: (1) disallow $3.2 million of questioned costs, (2) deobligate $1.3 million of project funding to be put to better use, and (3) instruct MEMA to accurately account for project costs.
(DA-11-12, April 2011, EMO)
http://www.oig.dhs.gov/assets%5CGrantReports%5COIG_DA-11-12_Apr11.pdf

City of Deerfield Beach, Florida
The city of Deerfield Beach, Florida, received a public assistance grant award totaling $13.9 million from the Florida Division of Emergency Management (FDEM), a FEMA grantee, for damages related to Hurricane Wilma, which occurred in October 2005. The award provided 100% FEMA funding for emergency protective measures, debris removal activities, and repairs to roads and facilities. We reviewed costs totaling $13.5 million claimed under 11 large projects. The city accounted for FEMA funds on a project-by-project basis according to federal regulations for large projects. However, the city's claim included $3.9 million of costs that were ineligible. We recommended that the Regional Administrator, FEMA Region IV, in coordination with FDEM, disallow the $3.9 million of ineligible costs.
(DA-11-13, April 2011, EMO)
http://www.oig.dhs.gov/assets%5CGrantReports%5COIG_DA-11-13_Apr11.pdf

North Carolina Department of Transportation – Disaster Activities Related to Tropical Storm Frances
The North Carolina Department of Transportation received a public assistance grant award totaling $12.2 million from the North Carolina Division of Emergency Management (NCDEM), a FEMA grantee, for damages related to Tropical Storm Frances, which occurred in September 2004. The award provided 75% FEMA funding for debris removal activities, emergency protective measures, road repairs, and replacement of bridges. The award consisted of 81 large projects and 337 small projects. We reviewed $5.3 million of costs under 12 large projects. Except for questioned costs of $63,095 (FEMA share $47,321) that resulted from ineligible overtime fringe benefits,

the Department properly accounted for and used FEMA funds. We recommended that the Regional Administrator, FEMA Region IV, in coordination with NCDEM, disallow the $63,095 (FEMA share $47,321) of questioned costs and review and determine the eligibility of overtime fringe benefit charges claimed for projects not included in the scope of our review.
(DA-11-14, April 2011, EMO)
http://www.oig.dhs.gov/assets%5CGrantReports%5COIG_DA-11-14_Apr11.pdf

North Carolina Department of Transportation – Disaster Activities Related to Hurricane Ivan
The North Carolina Department of Transportation received a public assistance grant award totaling $27.1 million from NCDEM, a FEMA grantee, for damages related to Hurricane Ivan, which occurred in September 2004. The award provided 75% FEMA funding for debris removal activities, emergency protective measures, road repairs, and replacement of bridges. We reviewed costs totaling $11.5 million under the disaster. The Department accounted for FEMA funds on a project-by-project basis according to federal regulations for large projects. However, we question $909,777 (FEMA share $682,333) of ineligible costs that resulted from duplication of benefits and excessive fringe benefits. We recommended that the Regional Administrator, FEMA Region IV, in coordination with NCDEM, disallow the $909,777 (FEMA share $682,333) of questioned costs and review and determine the eligibility of overtime fringe benefit charges claimed for projects not included in the scope of our review.
(DA-11-15, April 2011, EMO)
http://www.oig.dhs.gov/assets%5CGrantReports%5COIG_DA-11-15_Apr11.pdf

Coast Transit Authority
Coast Transit Authority (CTA) received a public assistance award of $8.2 million from MEMA, a FEMA grantee, for damages related to Hurricane Katrina in August 2005. The award provided 100% FEMA funding for emergency protective measures, and repair of buildings and equipment damaged as a result of the disaster. We reviewed $7.5 million awarded under five large projects. CTA's grant accounting system accounted for expenditures on a project-by-project basis and provided a means to readily trace project expenditures to source documents, as required by federal regulations. We identified $223,744 of project funding that should be deobligated and put to better use because the work authorized under the project was no longer required. Prior to issuance of the report, FEMA took action to deobligate the $223,744 of unneeded funding.
(DA-11-16, May 2011, EMO)
http://www.oig.dhs.gov/assets%5CGrantReports%5COIG_DA-11-16_May11.pdf

Florida International University
Florida International University received public assistance awards totaling $10.8 million from FDEM, a FEMA grantee, for damages related to Hurricanes Katrina and Wilma, which occurred August and October 2005, respectively. The awards provided 100% FEMA funding for emergency protective measures, debris removal activities, and repairs to roads and facilities. We reviewed costs totaling $9.4 million under the two disasters, which consisted of $689,987 under Hurricane Katrina and $8.7 million under Hurricane Wilma. The university accounted for FEMA funds on a project-by-project basis according to federal regulations for large projects. However, the university did not always comply with FEMA guidelines when awarding contracts for debris removal activities. Also, we questioned $927,446 of costs that were covered by insurance. We recommended that the Regional Administrator, FEMA Region IV: (1) instruct the university to comply with FEMA debris removal guidance when contracting for debris removal work under a FEMA award, and (2) disallow $927,446 of costs covered by insurance.
(DA-11-17, May 2011, EMO)
http://www.oig.dhs.gov/assets/GrantReports/OIG_DA-11-17_May11.pdf

City of Vero Beach, Florida – Disaster Activities Related to Hurricane Jeanne

The city of Vero Beach, Florida, received a public assistance award totaling $10.1 million from FDEM, a FEMA grantee, for damages related to Hurricane Jeanne, which occurred in September 2004. The award provided 100% FEMA funding for the first 72 hours of emergency protective measures and 90% funding thereafter. The award also provided 90% FEMA funding for debris removal activities and repairs to facilities and other public buildings. We reviewed costs totaling $7.8 million under the disaster. The city's accounting system did not separately account for large project expenditures on a project-by-project basis. We also identified $1.4 million (federal share $1.3 million) of ineligible and unsupported project costs. Additionally, the city did not always comply with FEMA guidelines and federal regulations when contracting for debris removal activities. We recommended that the Regional Administrator, FEMA Region IV: (1) instruct the city, for future declarations, to account for FEMA funding on a project-by-project basis; (2) disallow $1.4 million of questioned costs; and (3) instruct the city, for future declarations, to comply with federal regulations and FEMA guidelines governing contracting practices.
(DA-11-18, May 2011, EMO)
http://www.oig.dhs.gov/assets%5CGrantReports%5COIG_DA-11-18_May11.pdf

City of Vero Beach, Florida – Disaster Activities Related to Hurricane Frances

The city of Vero Beach, Florida, received a public assistance award totaling $9.6 million from FDEM, a FEMA grantee, for damages related to Hurricane Frances, which occurred in September 2004. The award provided 100% FEMA funding for the first 72-hours of emergency protective measures and 90% funding thereafter. The award also provided 90% FEMA funding for debris removal activities and repairs to facilities and other public buildings. We reviewed costs totaling $8.3 million under the disaster. The city's accounting system did not separately account for project expenditures on a project-by-project basis. We also identified $2.6 million (federal share $2.3 million) of ineligible and unsupported project costs. Additionally, the city did not always comply with FEMA guidelines and federal regulations when contracting for debris removal activities. We recommended that the Regional Administrator, FEMA Region IV: (1) instruct the city, for future declarations, to account for FEMA funding on a project-by-project basis; (2) disallow $2.6 million of questioned costs; and (3) instruct the city, for future declarations, to comply with federal regulations and FEMA guidelines governing contracting practices.
(DA-11-19, May 2011, EMO)
http://www.oig.dhs.gov/assets%5CGrantReports%5COIG_DA-11-19_May11.pdf

FEMA Public Assistance Grant Funds Awarded to Gulf Shores Utilities, Gulf Shores, Alabama

Gulf Shores Utilities in Gulf Shores, Alabama, received a public assistance grant award totaling $7.6 million from the Alabama Emergency Management Agency (AEMA), a FEMA grantee, for damages related to Hurricane Ivan, which occurred in September 2004. The award provided 100% FEMA funding for the first 72 hours of debris removal and emergency protective measures undertaken during the disaster, and 90% funding thereafter. The award also provided 90% FEMA funding for repairs to facilities and other public buildings. We reviewed $7.4 million of costs under four large projects. We determined the Utility accounted for and expended FEMA funds according to federal regulations and FEMA guidelines.
(DA-11-20, August 2011, EMO)
http://www.oig.dhs.gov/assets/GrantReports/OIG_DA-11-20_Aug11.pdf

FEMA Public Assistance Grant Funds Awarded to Memorial Hospital at Gulfport, Mississippi

Memorial Hospital at Gulfport, in Gulfport, Mississippi, received an award of $8.3 million from MEMA, a FEMA grantee, for damages related to Hurricane Katrina. The award provided 100% FEMA funding for debris removal, emergency protective measures, and repairs to damaged buildings and equipment. Our audit focused on $7.7 million awarded under five large projects. The hospital's grant accounting system did not

account for expenditures on a project-by-project basis. We also determined that the hospital's allocation of insurance recoveries among FEMA eligible and ineligible damages may have resulted in a disproportionate share being allocated to reduce FEMA project costs. We recommended that the Regional Administrator, FEMA Region IV: (1) instruct the hospital to separately account for project costs, and (2) evaluate the hospital's allocation of insurance proceeds for consistency with FEMA guidelines and reduce FEMA project costs, as appropriate.
(DA-11-21, August 2011, EMO)
http://www.oig.dhs.gov/assets/GrantReports/OIG_DA-11-21_Aug11.pdf

FEMA Public Assistance Grant Funds Awarded to the City of Mobile, Alabama
The city of Mobile, Alabama, received a public assistance award totaling $5.3 million from AEMA, a FEMA grantee, for damages resulting from Hurricane Katrina, which occurred in August 2005. The award provided 100% FEMA funding for debris removal and emergency protective measures. We reviewed costs totaling $3.5 million claimed under seven large projects. We determined that the city accounted for and expended FEMA funds according to federal regulations and FEMA guidelines.
(DA-11-22, August 2011, EMO)
http://www.oig.dhs.gov/assets/GrantReports/OIG_DA-11-22_Aug11.pdf

FEMA Public Assistance Grant Funds Awarded to Gulf Coast Community Action Agency, Gulfport, Mississippi
The Gulf Coast Community Action Agency received a public assistance award of $5.6 million from MEMA, a FEMA grantee, for damages resulting from Hurricane Katrina, which occurred in August 2005. The award provided 100% FEMA funding for debris removal and repair/replacement of damaged buildings and equipment. Our audit focused on $5.6 million awarded under 15 projects. The agency did not account for project expenditures on a project-by-project basis, as required by federal regulations. Also, the agency did not always comply with FEMA guidelines and federal regulations when procuring services under the award. Finally, we identified $2.3 million of unneeded project funding, and $2.7 million of duplicate benefits. We recommended that the Regional Administrator, FEMA Region IV: (1) instruct the agency to account for large projects on a project-by-project basis, (2) instruct the Agency to comply with federal procurement regulations, (3) deobligate and put to better use $2.3 million of unneeded project funding, and (4) disallow $2.7 million of duplicate benefits.
(DA-11-23, August 2011, EMO)
http://www.oig.dhs.gov/assets/GrantReports/OIG_DA-11-23_Aug11.pdf

FEMA Public Assistance Grant Funds Awarded to Wayne County, Mississippi, Board of Supervisors
The Wayne County, Mississippi, Board of Supervisors received a public assistance award of $25.6 million from MEMA, a FEMA grantee, for damages related to Hurricane Katrina. The award provided 100% FEMA funding for debris removal, emergency protective measures, and permanent repairs to damaged facilities. Our audit focused on $24.3 million awarded under three large projects. The county did not account for large project expenditures on a project-by-project basis, and did not always follow federal procurement regulations when awarding and monitoring contracts for debris removal activities. We also identified $4.6 million of ineligible costs for debris removed from private property, and a $2.7 million overpayment of FEMA funds. We recommended that the Regional Administrator, FEMA Region IV: (1) instruct the county to separately account for large projects, (2) instruct the county to comply with federal procurement regulations, (3) disallow $4.6 million of ineligible costs, (4) disallow the $2.7 million overpayment, and (5) instruct the county to comply with contract monitoring requirements.
(DA-11-24, September 2011, EMO)
http://www.oig.dhs.gov/assets/audit/OIG_DA-11-24_Sep11.pdf

Xavier University of Louisiana
Xavier University of Louisiana received a $75.4 million award for damages resulting from Hurricane Katrina. The award provided 100% FEMA funding for 40 large and 57 small

projects. Our review determined that Xavier did not account for and expend FEMA grant funds according to federal regulations and FEMA guidelines. Xavier did not account for costs on a project-by-project basis as required and provided documentation that included duplicate, ineligible, and unsupported costs. Further, Xavier did not follow federal procurement standards and did not purchase the required property insurance. We recommended that FEMA disallow the entire claim of $75.4 million in unsupported or ineligible. This amount also includes $59.4 million of improperly awarded contract costs, $281,430 of ineligible costs claimed for uninsured damages, and $12,291 ineligible costs claimed for facilities that Xavier did not own. We also recommended that FEMA complete the insurance review and allocate applicable insurance proceeds to Xavier's projects (approximately $14.7 million).
(DD-11-12, April 2011, EMO)
http://www.oig.dhs.gov/assets%5CGrantReports%5COIG_DD-11-12_Apr11.pdf

City of Austin, Texas
The city of Austin, Texas, received an award of $11.6 million for two Hazard Mitigation Grant Programs (HMGP) projects following Hurricane Rita and an extreme wildfire threat to acquire and remove residential properties to mitigate against future losses. The city claimed $10.4 million in direct project costs. Our audit determined that the city's project management generally complied with applicable regulations and guidelines. However, the city did not always account for FEMA funds according to federal regulations and FEMA guidelines, and one project did not meet FEMA HMGP eligibility requirements. Therefore, we recommended that the Regional Administrator, FEMA Region VI, disallow $235,479 ($176,609 federal share) in ineligible indirect force account labor costs, and $596,150 ($447,113 federal share) as ineligible costs because Project 1624-28 did not meet HMGP eligibility requirements.
(DD-11-13, April 2011, EMO)
http://www.oig.dhs.gov/assets%5CGrantReports%5COIG_DD-11-13_Apr11.pdf

South Central Power Company, Ohio
South Central Power Company, Ohio (SCP), received an award of $11.8 million from the Ohio Emergency Management Agency (Ohio EMA), a FEMA grantee, for damages caused by severe winter storms, flooding, and mudslides on December 22, 2004, through February 1, 2005. SCP generally accounted for and expended FEMA grant funds according to federal regulations and FEMA guidelines. However, SCP claimed $117,951 in mutual aid costs incurred in completing permanent recovery work, which is not eligible according to FEMA policy. We recommended that the Regional Administrator, FEMA Region V, disallow $117,951 in ineligible mutual aid costs.

FEMA is reviewing its policy and plans to address the eligibility of Category F work performed under mutual aid. The grantee has requested a waiver of FEMA's mutual aid policy.
(DD-11-14, April 2011, EMO)
http://www.oig.dhs.gov/assets%5CGrantReports%5COIG_DD-11-14_Apr11.pdf

FEMA Public Assistance Grant Funds Awarded to Saint Mary's Academy, New Orleans, Louisiana
St. Mary's Academy (SMA), in New Orleans, Louisiana, received an award of $56.4 million for damages resulting from Hurricane Katrina, which occurred in August 2005. SMA accounted for funds on a project-by-project basis. However, SMA did not comply with federal procurement standards in awarding contracts, and it did not fully insure the cost of a new facility. Additionally, FEMA had not completed allocation of insurance proceeds to SMA's projects.

We recommended the Regional Administrator, FEMA Region VI, disallow $18.4 million of ineligible contract costs and $31.2 million of ineligible, uninsured facility costs. We also recommended that FEMA allocate $1.5 million of insurance proceeds to SMA's projects.
(DD-11-15, August 2011, EMO)
http://www.oig.dhs.gov/assets/GrantReports/OIG_DD-11-15_Aug11.pdf

Interim Report on FEMA Public Assistance Grant Funds Awarded to Regional Transit Authority, New Orleans, Louisiana

At the time of this interim report, we were auditing $87.73 million of the $123.9 million of FEMA public assistance funds awarded to the New Orleans Regional Transit Authority (RTA) for disaster recovery work related to Hurricane Katrina. The purpose of this report was to advise FEMA of two issues that required immediate attention. First, neither RTA nor FEMA had provided adequate documentation to verify RTA's legal responsibility for 151 leased buses damaged as a result of the disaster. Second, RTA officials had not provided us with requested insurance policies for the buses and schedules of property insured. Therefore, we could not determine the eligibility of the $31.74 million that FEMA anticipated funding for the 151 damaged buses. We recommended that the Regional Administrator, FEMA Region VI: (1) disallow $31.74 million as unsupported funding anticipated for the repair or replacement of 151 leased buses, or provide proof that RTA was legally responsible for the 151 buses at the time of the disaster, and (2) require RTA to provide any and all insurance policies; schedules of properties to include year, make, model, and Vehicle Identification Number; and related supporting documentation for all RTA-owned and leased buses.
(DD-11-16, August 2011, EMO)
http://www.oig.dhs.gov/assets/GrantReports/OIG_DD-11-16_Aug11.pdf

Capping Report: FY 2010 FEMA Public Assistance Grant and Subgrant Audits

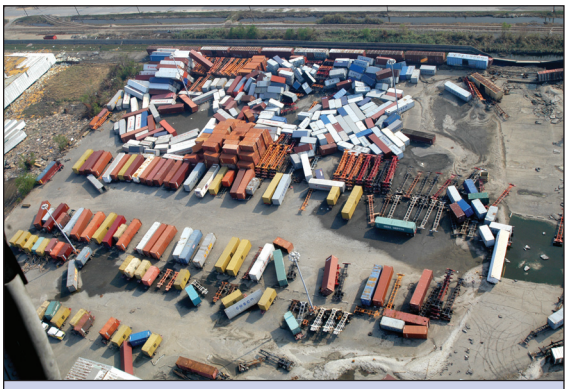
This report summarizes the results of Public Assistance (PA) program grant and subgrant audits performed during FY 2010. We reviewed audit findings and recommendations made to FEMA officials as they related to PA program funds awarded to state, local, and tribal governments and eligible nonprofit organizations. In FY 2010, we issued 45 audit reports on grantees and subgrantees awarded FEMA PA funds between July 2003 and October 2008 as a result of 29 presidentially declared disasters in 16 states and 2 U.S. territories. The subgrantees were awarded $2.29 billion in project funding for debris removal; emergency protective measures; or permanent repair, restoration, and replacement of damaged facilities. We audited $1.23 billion of the $2.29 billion, or 54% of the awarded amounts. Of the 45 audits performed in FY 2010, 44 reports contained 155 recommendations regarding 152 findings or reportable conditions resulting in a potential monetary benefit of $165.25 million. This amount included $104.48 million in project costs questioned as ineligible or unsupported that should be disallowed and $60.77 million in funds that were unused or uncollected that should be put to better use.
(DD-11-17, August, EMO)
http://www.oig.dhs.gov/assets/GrantReports/OIG_DD-11-17_Aug11.pdf

FEMA Public Assistance Grant Funds Awarded to Iowa Department of Transportation

The Iowa Department of Transportation (DOT) generally accounted for and expended FEMA grant funds according to federal regulations and FEMA guidelines. However, we questioned $48,440 because Iowa DOT's claim included $31,919 of ineligible costs not related to the disaster and $16,521 of duplicate costs claimed under a concurrent disaster. Iowa DOT received an award of $3.3 million from the Iowa Homeland Security and Emergency Management Division, a FEMA grantee, for damages caused by severe winter storms from February 23 to March 2, 2007. The award provided 75% FEMA funding for six large projects. We recommended that the Regional Director, FEMA Region VII, disallow $31,919 ($23,939 federal share) of ineligible force account costs that are not related to the disaster and disallow $16,521 ($12,391 federal share) of duplicate force account labor costs.
(DD-11-18, August 2011, EMO)
http://www.oig.dhs.gov/assets/GrantReports/OIG_DD-11-18_Aug11.pdf

FEMA Public Assistance Grant Funds Awarded to Port of New Orleans, Louisiana

Port of New Orleans (PONO) accounted for and expended FEMA grant funds according to federal regulations and FEMA guidelines; and its plan for completing 14 improved projects appears reasonable. However, PONO has not completed the allocation of insurance proceeds to its projects and did not use all approved funding in completing certain projects. As a result, FEMA should allocate approximately $2.6 million of insurance proceeds to PONO's projects and disallow those amounts from the projects as ineligible, and deobligate $670,974 in approved project costs that exceeded the actual amounts incurred and claimed. In addition, Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP) overpaid PONO $1.4 million; however, we did not question these costs because FEMA funding was not involved. (DD-11-19, August 2011, EMO)
http://www.oig.dhs.gov/assets/audit/OIG_DD-11-19_Aug11.pdf

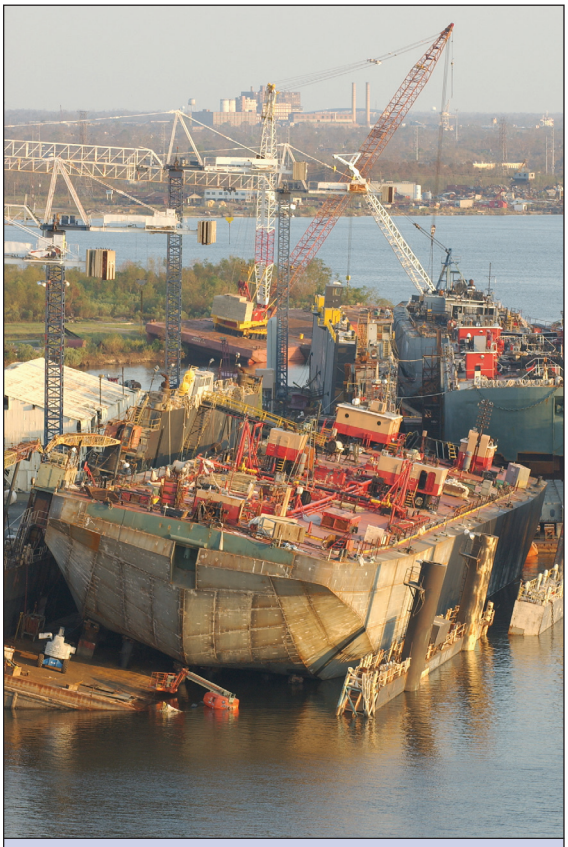


New Orleans, September 20, 2005 - Shipping containers at the Port of New Orleans are tossed about a staging area.
Source: FEMA Photo Library

FEMA Public Assistance Grant Funds Awarded to Calcasieu Parish School Board, Lake Charles, Louisiana

Calcasieu Parish School Board (CPSB) received an award of $14.7 million from GOHSEP, a FEMA grantee, for damages resulting from Hurricane Rita. CPSB accounted for FEMA grant funds on a project-by-project basis according to federal regulations. However, CPSB did not follow federal procurement standards in awarding $11.1 million of disaster-related contracts; and its claim included ineligible and unsupported costs.

We recommended that the Regional Administrator, FEMA Region VI, disallow $3.1 million of improperly procured and ineligible contract costs and $22,610 of unsupported contract costs. Additionally, we recommended that FEMA deobligate $747,106 of unused funds to put those federal funds to better use and allocate $545,077 of insurance proceeds to CPSB projects to reduce those amounts from the projects as ineligible. (DD-11-20, September 2011, EMO)
http://www.oig.dhs.gov/assets/audit/OIG_DD-11-20_Sep11.pdf



A large ship in a port outside the city of New Orleans is damaged as result of Hurricane Katrina.
Source: FEMA Photo Library

FEMA Public Assistance Grant Funds Awarded to Jesuit High School, New Orleans, Louisiana

Jesuit High School, New Orleans, Louisiana, received an award of $11.5 million for damages resulting from Hurricane Katrina, which occurred in August 2005. Jesuit accounted for funds on a project-by-project basis. However, Jesuit did not comply with federal procurement standards in awarding contracts, and its claim included ineligible contract costs, unsupported contract costs, and duplicate funding. Additionally, FEMA has not completed allocation of insurance proceeds to Jesuit's projects and should deobligate and put to better use unused federal funds.

We recommended that the Regional Administrator, FEMA Region VI, disallow $11.6 million of ineligible and unsupported costs, complete the insurance review and allocate applicable insurance proceeds to Jesuit's projects, and deobligate and put to better use $27,519 of unused federal funds. (DD-11-21, September 2011, EMO)
http://www.oig.dhs.gov/assets/GrantReports/OIG_DD-11-21_Sep11.pdf

FEMA Public Assistance Grant Funds Awarded to Henderson County, Illinois

Henderson County, IL received a $4.8 million award for damages caused by severe storms and flooding during June and July 2008. The county did not account for and expend FEMA grant funds according to federal regulations and FEMA guidelines resulting in $3.7 million of ineligible costs. The county did not follow federal procurement standards for two contracts totaling $3.6 million and did not complete demolition work on 23 small projects totaling $48,728. We recommended that FEMA disallow the $3.7 million of ineligible costs.
(DD-11-22, September 2011, EMO)
http://www.oig.dhs.gov/assets/GrantReports/OIG_DD-11-22_Sep11.pdf

FEMA Region VI Audit Follow-up and Resolution Activities

As of March 31, 2011, 27 of the 61 audit reports the Central Regional Office issued to FEMA Region VI between July 2004 and September 2010 remained open. The Region's audit follow-up and resolution activities for the 27 audit reports exceeded timeframes established by OMB Circular A-50, and DHS Directive 077-01. Specifically FEMA did not—

1. Respond to 25 audit reports within the established timeframes set forth in the final report,
2. Reach resolution on 114 of 156 recommendations within a 6-month timeframe, or
3. Implement agreed-upon corrective actions in 95 of 156 recommendations within 1 year of the final report issue date.

As a result, FEMA missed or delayed opportunities to improve the effectiveness and efficiency of government operations and has not promptly addressed more than $60 million in questioned costs within a year after we issued our reports. We recommended that the Region: (1) develop and implement a follow-up system that meets the requirements of OMB Circular A-50 and DHS Directive 077-01, and (2) assign the necessary resources to ensure the proper resolution and implementation of audit recommendations within established timeframes.
(DD-11-23, September 2011, EMO)
http://www.oig.dhs.gov/assets/GrantReports/OIG_DD-11-23_Sep11.pdf

FEMA Public Assistance Grant Funds Awarded to Orleans Parish Criminal Sheriff's Office, Louisiana

Orleans Parish Criminal Sheriff's Office (OPCSO) accounted for and expended FEMA grant funds on a project-by-project basis as required by federal regulations. However, OPCSO did not always expend the funds according to federal regulations and FEMA guidelines. As a result, we question $3.5 million of ineligible and unsupported costs that OPCSO claimed. In addition, FEMA should deobligate and put to better use $285,771 in federal funds that exceeded the actual amounts OPCSO incurred and claimed.
(DD-11-24, September 2011, EMO)
http://www.oig.dhs.gov/assets/GrantReports/OIG_DD-11-24_Sep11.pdf

Reclamation District 768, Arcata, California

We audited PA funds awarded to Reclamation District 768, in Arcata, California. District officials did not comply with federal regulations and FEMA guidelines when procuring professional services and disaster repairs totaling $2.1 million ($1.6 million federal share). This amount includes $844,893 for professional services costs that were excessive and unreasonable. Further, after completing all disaster-related projects, the district had a remaining unused award amount of $1.9 million ($1.4 million federal share) that should be deobligated and put to better use.

We recommended that the FEMA Region IX Administrator, in coordination with the grantee: (1) disallow $1.2 million (federal share $932,305) of ineligible contract costs incurred without compliance with federal procurement regulations and FEMA guidelines (this amount is net of the $844,893 recommended for disallowance in Recommendation #2); (2) disallow $844,893 (federal share $633,670) of engineering, design, and project management costs that were ineligible as excessive and unreasonable, and incurred without compliance with federal procurement regulations and FEMA guidelines; and (3) deobligate $1.9 million (federal share $1.4 million) and put those funds to better use.
(DS-11-09, July 2011, EMO)
http://www.oig.dhs.gov/assets/GrantReports/OIG_DS-11-09_Jul11.pdf

FEMA Public Assistance Grants Awarded to County of Humboldt, California

We audited PA funds awarded to the county of Humboldt, California. County officials did not account for and expend $895,535 according to federal regulations and FEMA guidelines, and have unused funds that should be deobligated. Specifically, we identified: (1) $740,000 in improper procurement costs, (2) $234,013 of funds not used, (3) $139,382 in ineligible contract overpayments and improper procurement costs, and (4) $16,153 in ineligible force account labor costs. This report also addresses ineligible force account equipment charges, and the county's net small project overrun.

We recommended that the FEMA Region IX Administrator, in coordination with the grantee: (1) disallow $740,000 (federal share $555,000) in ineligible contracting costs incurred without compliance with federal procurement regulations and FEMA guidelines (this amount is net of the $139,382 recommended for disallowance in Recommendation #3); (2) deobligate $234,013 (federal share $175,510) and put those funds to better use; (3) disallow $139,382 (federal share $104,537) in ineligible, excessive contract charges and incurred without compliance with federal procurement regulations and FEMA guidelines; (4) disallow $16,153 (federal share $12,115) in ineligible force account labor costs; (5) ensure that county officials claim the lowest eligible rates for force account equipment charges; and (6) ensure that county officials claim only eligible costs in their net small project overrun.
(DS-11-10, August 2011, EMO)
http://www.oig.dhs.gov/assets/GrantReports/OIG_DS-11-10_Aug11.pdf

FEMA Public Assistance Grants Awarded to City of Petaluma, California

We audited PA funds awarded to the city of Petaluma, California. The city generally expended and accounted for FEMA funds according to federal regulations and FEMA guidelines. However, the city did not use $2.2 million of FEMA-approved funds; therefore, FEMA should deobligate those federal funds and put them to better use. Also, city officials planned to request reimbursement for costs FEMA had not yet

approved and, for one project, spent significantly more than the approved amount without notifying FEMA about the increases.

We recommended that the FEMA Region IX Administrator, in coordination with the grantee: (1) deobligate $1.2 million (federal share $876,547) for permanent work to dispose of sediment and put those federal funds to better use; (2) deobligate $1 million (federal share $752,839) for emergency debris dredging and disposal and put those federal funds to better use; and (3) ensure that the city claims only authorized and eligible disaster costs. (DS-11-11, September 2011, EMO)
http://www.oig.dhs.gov/assets/audit/OIG_DS-11-11_Sep11.pdf

FEMA Public Assistance Grant Funds Awarded to City of Paso Robles, California
We audited PA grant funds awarded to the city of Paso Robles, California. City officials did not comply with federal regulations and FEMA guidelines for $1.1 million in project charges. Specifically, we identified: (1) $559,788 in improper procurement costs; (2) $456,157 in unreasonable (excessive) costs for construction management, architectural and engineering (A&E), and design services; (3) $43,125 in costs not included in the FEMA-approved scope of work; and (4) $51,882 in unsupported costs.

We recommended that the FEMA Region IX Administrator, in coordination with the California Emergency Management Agency (Cal EMA), disallow: (1) $559,788 (federal share $419,841) in ineligible contract costs charged to Projects 194 and 249 (this amount is net of the $456,157 recommended for disallowance in Recommendation #2); (2) $456,157 (federal share $342,118) in ineligible costs for construction management, A&E, and design services for Projects 194 and 249 that were unreasonable and noncompliant with federal procurement regulations and FEMA guidelines; (3) $43,125 (federal share $32,344) in ineligible project costs not included in the FEMA-approved scope of work for Project 224; and (4) $51,882 (federal share $38,912) in unsupported costs for Projects 189 and 224. (DS-11-12, September 2011, EMO)
http://www.oig.dhs.gov/assets/audit/OIG_DS-11-12_Sep11.pdf

FEMA Public Assistance Grant Funds Awarded to County of Sonoma, California
We audited PA grant funds awarded to county of Sonoma, California, for FEMA Disaster Number 1646-DR-CA. County officials generally expended and accounted for FEMA funds according to federal regulations and FEMA guidelines. However, we identified: (1) $1.2 million of unused federal funds that should be put to better use; (2) $521,355 of ineligible project costs; and (3) $1,176 in unsupported duplicate project charges.

We recommended that the FEMA Region IX Administrator, in coordination with Cal EMA: (1) deobligate $1.2 million (federal share $906,815) and put those unused funds to better use; (2) disallow $521,355 (federal share $391,016) in ineligible costs for Project 225; and (3) disallow $1,176 (federal share $882) in unsupported duplicate charges for Project 628. (DS-11-13, September 2011, EMO)
http://www.oig.dhs.gov/assets/GrantReports/OIG_DS-11-13.pdf

INVESTIGATIONS

Disaster Assistance Recipient Convicted of False Claims of $14,246
We investigated a disaster benefit recipient who submitted a false claim to FEMA that his residence in Mississippi was damaged by Hurricane Katrina. The subject was not living in the claimed residence at the time the hurricane occurred. He had obtained $14,246 in disaster assistance funds that he was not entitled to receive. He was arrested, convicted of the theft, sentenced to 16 months incarceration, 36 months probations, and 60 hours of community service.

FEMA Disaster Recipient Sentenced for Fraudulent Claims for Tax Refunds

We investigated an individual who filed multiple false claims for FEMA disaster assistance allowing her to receive three checks in her name for a total of $4,938. The recipient lived in three different locations in Texas, and falsely claimed damage caused by Hurricane Katrina. In addition, she defrauded the Internal Revenue Service of at least $300,000 by preparing and filing false tax returns on behalf of other people. She was sentenced to 42 months incarceration and ordered to pay restitution in the amount of $4,938 with a fine of $75,000.

Road Home Benefit Recipient Pleads Guilty to $102,718 in Fraud

We conducted a joint investigation with the HUD OIG concerning a New Orleans resident who defrauded FEMA and HUD of approximately $102,718 in funds from The Road Home Program. The subject alleged damage for a property she was not residing in at the time of Hurricane Katrina; in addition, a FEMA travel trailer was also leased out to the subject and placed on her property. The subject pleaded guilty to Theft of Government Funds and was sentenced to 3 years probation. The subject was ordered to pay full restitution to the government.

County Supervisor Hides Bribe Money under Kitchen Sink

We conducted an investigation concerning a government contract for debris removal in Mississippi after Hurricane Katrina. It was alleged that the contractors agreed to pay certain county supervisors cash per cubic yard of debris that was removed in order to obtain the debris removal contract. Our investigation determined that a county supervisor from Mississippi and several of his fellow supervisors had accepted these cash bribes to influence contract awards. The county received more than $13,000,000 in FEMA grants for reconstruction after Hurricane Katrina. During the investigation, agents recovered $17,500 in bribe money concealed under the county supervisor's kitchen sink. The subject was sentenced to 78 months incarceration, 36 months probation, and $18,480 in restitution.

Two Convicted for Conspiracy to Fraudulently Obtain $750,000 in FEMA Funds

We conducted an investigation concerning two individuals who conspired to fraudulently obtain more than $750,000 in FEMA disaster assistance funds. One of the conspirators directly received more than $88,232 in eight separate bank accounts after making fraudulent claims. The subjects pleaded guilty to the fraud scheme. One subject was sentenced to 28 months confinement, 36 months probation, and ordered to pay restitution of the full amount to FEMA. The second subject was sentenced to 7 months confinement, 36 months of probation, and ordered to pay restitution of $50,875.

Man Convicted of Stealing FEMA Contract Award Funds

We conducted an investigation that involved an allegation from FEMA questioning a $70,000 bill submitted by a contractor for tree removal. The investigation determined that the subject conspired with other contractors to submit inflated expense vouchers to FEMA for debris removal associated with the Hurricane Katrina cleanup. The subject pleaded guilty to stealing more than $50,000 in FEMA contract award funds. Sentencing is pending.

U.S. Government Employees Conspire to Defraud the Government

We worked a case in conjunction with the Small Business Administration (SBA) OIG, involving a DHS contract security guard and a relative who was an SBA employee in Dallas, Texas. Our investigation revealed that the two individuals conspired to create and submit fraudulent SBA loan documents and subsequently defaulted on a $171,600 fraudulent government loan. Sentencing is pending.

Anonymous Tip Leads to FEMA Fraud Conviction

We investigated an individual who made a FEMA individual cash assistance claim for items damaged by Hurricane Ike and Hurricane Katrina. An anonymous tip led to the investigation. The subject claimed damage to her primary residence and personal property, including her washer, dryer,

refrigerator, and stove. She provided FEMA inspectors with false addresses to which assistance benefits were sent. The subject pleaded guilty to Mail and Wire Fraud, and on August 4, 2011, was sentenced to 21 months incarceration, 3 years supervised release, and restitution of $30,700 to FEMA, and a special assessment of $800.

Double Dipping of Assistance Funds Leads to Fraud Arrest

We conducted an investigation along with the HUD OIG of an individual who had submitted fraudulent claims for damage caused by Hurricane Katrina. The investigation determined that the subject claimed damage loss to FEMA for disaster assistance funds and to HUD for Section 8 for rental assistance. The subject received the fraudulent assistance, which caused a total loss amount of $33,523. The subject was arrested, convicted, and is pending sentencing.

Former Mayor and Employees Defrauding FEMA

As a result of our investigation, the former mayor, police chief, and three other city employees from Ball, Louisiana, pleaded guilty to fraud charges related to FEMA funds dispersed after Hurricane Gustav. The mayor and others defrauded the government by overstating the hours worked and the mileage on town vehicles and equipment used in response to Hurricane Gustav in 2008 and later submitted falsified timesheets to FEMA for reimbursement. All five individuals have pleaded guilty and are awaiting sentencing. The former mayor and police chief face a maximum sentence of 5 years in prison and $250,000 in fines.

UPDATE: The former mayor was ordered to pay $105,566 in restitution and a $25,000 fine for his role in defrauding FEMA. He was sentenced to 48 months in federal prison with 3 years of supervised release, and 200 hours of community service. The four other co-conspirators were sentenced to probation and community service.

U.S. Postal Service Worker Defrauds Three Government Agencies

We conducted an investigation of a U.S. Postal Service worker based upon an allegation of disaster fraud. The subject submitted false claims for disaster benefits to FEMA, HUD, and the SBA, receiving in excess of $160,000 in funds. The subject pleaded guilty and received 3 years of probation and was ordered to pay restitution of $46,300, and a $100 special assessment.

FEMA Representative and Applicant Guilty of Defrauding FEMA of $700,000

We conducted an investigation of a fraud scheme involving an individual applicant and a FEMA representative. Our investigation determined that the subject and the FEMA employee conspired to commit fraud against FEMA of approximately $700,000 by submitting numerous Hurricane Katrina disaster assistance applications. The subjects pleaded guilty to defrauding FEMA of approximately $700,000 and were sentenced to 11 months incarceration, 36 months probation, 70 hours of community service, and $27,687 in restitution.

Former General Manager of New Orleans Railroad Pleads Guilty of Theft

We investigated a former employee of the New Orleans Public Belt Railroad for misappropriating FEMA funding destined for the Public Belt Railroad. Between 2007 and 2010, the former employee unlawfully misapplied monies and assets from the New Orleans Public Belt Railroad for personal gain. The subject admitted to spending at least $5,600 of government funds for personal and entertainment expenses, and pleaded guilty to theft and misapplication of federal funds. Sentencing is pending, and he faces a maximum of 10 years in prison and a fine of $250,000.

FEDERAL LAW ENFORCEMENT TRAINING CENTER

MANAGEMENT REPORTS

Information Technology Management Letter for the Federal Law Enforcement Training Center Component of the FY 2010 DHS Financial Statement Audit

KPMG LLP, under contract with DHS OIG, conducted the audit of the Federal Law Enforcement Training Center (FLETC) consolidated balance sheet in support of DHS' financial statement audit as of September 30, 2010. As part of this review, KPMG LLP noted certain matters involving internal control and other operational matters with respect to IT and have documented its comments and recommendation in the Information Technology Management Letter. The overall objective of our audit was to evaluate the effectiveness of IT general controls of FLETC's financial processing environment and related IT infrastructure. KPMG LLP noted that FLETC took corrective action to address many prior years' IT control weaknesses. However, during FY 2010, KPMG LLP continued to find IT general control weaknesses at FLETC. The most significant weaknesses from a financial statement audit perspective related to controls over access and configuration management and the weaknesses in physical security and security awareness. Collectively, the IT control weaknesses limit FLETC's ability to ensure that critical financial and operational data are maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively impact the internal controls over FLETC's financial reporting and its operation, and KPMG LLP considers them to collectively represent a material weakness under standards established by AICPA.
(OIG-11-76, April 2011, ITA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-76_Apr11.pdf

FEDERAL PROTECTIVE SERVICE

INVESTIGATIONS

Contracting Officer Takes Bribes in Exchange for Armed Guard Contract

We received an allegation that a COTR with the Federal Protective Service (FPS), Fort Lauderdale, Florida, accepted paid trips to Houston, Texas, from the owner of a company that provided armed security guards to the FPS. The COTR received vacation trips and a promise of future employment in exchange for assisting the company in obtaining service contracts in the Houston area. The COTR's actions resulted in the company being awarded an FPS contract valued at $1,974,915. The COTR pleaded guilty to conspiracy related to bribery and was sentenced to 3 years probation. The convicted COTR was also debarred from involvement in federal contracting for 5 years.

Contract Employee Falsifies Armed Guard Training Records

We received an allegation involving a contract company that provided armed security gurards for FPS. The subject of the allegation, a contract employee, provided false and fictitious training records to FPS in an effort to satisfy requirements of the contract. The contract guaranteed that all guards were to successfully complete firearms training and American Red Cross standardized training for cardiopulmonary resuscitation, the use of an automated external defibrillator, and first aid in order to be considered qualified to stand post. The subject of the allegation admitted to intentionally falsifying certifications for the security guards in order to make it appear that they were in compliance with the contract. Federal prosecution of the subject was declined; however, the subject was debarred for a 6-month period of time beginning June 15, 2011.

OFFICE FOR CIVIL RIGHTS AND CIVIL LIBERTIES

We received 547 civil rights and civil liberties complaints from April 1, 2011 through September 30, 2011. Of those, we opened 8 investigations and referred 536 complaints to the Department's Office for Civil Rights and Civil Liberties or other component agencies. OIG is also reviewing the remaining three complaints to determine whether the complaints should be referred or opened for DHS OIG investigation.

OFFICE OF INTELLIGENCE AND ANALYSIS

MANAGEMENT REPORTS

Management Oversight and Additional Automated Capabilities Needed to Improve Intelligence Information Sharing

DHS has taken actions to create an environment and infrastructures necessary to promote intelligence information sharing. Specifically, the Office of Intelligence and Analysis (I&A) is responsible for leading and managing the DHS Intelligence Enterprise and establishing a unified, coordinated, and integrated intelligence program for the Department. Additionally, I&A established the various councils, boards, and a task force to serve as forums for the components' leadership and offices to collaborate on information sharing initiatives and to address information sharing issues. Further, components are developing intelligence information sharing systems to improve communication with their field offices and other DHS components.

We recommended that the Department improve its intelligence information sharing capabilities to ensure that components have the relevant data, policies, and information systems to perform their missions. DHS needs to provide additional management oversight to improve the effectiveness of the intelligence information sharing process. Specifically, DHS needs to finalize its policies and procedures to clarify and promote intelligence information sharing across the Department.

Finally, DHS needs to improve enterprise-wide intelligence information system sharing capabilities to ensure that threat and vulnerability information is readily available to provide a timely response. (OIG-11-87, June 2011, ITA)
http://www.oig.dhs.gov/assets/Mgmt/OIGr_11-87_Jun11.pdf

TRANSPORTATION SECURITY ADMINISTRATION

MANAGEMENT REPORTS

Information Technology Management Letter for the Transportation Security Administration Component of the FY 2010 DHS Financial Statement Audit

KPMG LLP, under contract with DHS OIG, conducted an audit of DHS' consolidated balance sheet as of September 30, 2010, and the related statement of custodial activity. KPMG LLP performed an evaluation of information technology general controls (ITGC) at the Transportation Security Administration (TSA) to assist in planning and performing the audit. As part of this review, KPMG LLP noted certain matters involving internal control and other operational matters with respect to IT and documented its comments and recommendation in the Information Technology Management Letter. The overall objective of our audit was to evaluate the effectiveness of IT general controls of TSA's financial processing environment and related IT infrastructure. KPMG LLP noted that TSA took corrective action to address many prior years' IT control weaknesses. However, during FY 2010, KPMG LLP continued to find IT general control weaknesses at TSA. The most significant weaknesses from a financial statement audit perspective related to controls over the development, implementation, and tracking of scripts at Coast Guard's Finance Center. Collectively, the IT control deficiencies limited TSA's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these deficiencies negatively impacted the internal controls over TSA financial reporting and

its operation, and KPMG LLP considers them to collectively represent a significant deficiency under standards established by AICPA.
(OIG-11-73, April 2011, ITA)
http://www.oig.dhs.gov/assets%5CMgmt%5COIG_11-73_Apr11.pdf

DHS Grants Used for Mitigating Risks to Amtrak Rail Stations
DHS grant recipients, such as Amtrak, transit agencies, and state and local authorities, coordinate risk mitigation projects at Amtrak high-risk rail stations to prevent duplication and avoid uneconomical use of grant funds. However, at the four rail stations visited, we identified that Amtrak did not mitigate critical vulnerabilities reported in DHS-funded risk assessments. Although many factors contributed to Amtrak's unaddressed station vulnerabilities, the primary causes were that TSA did not require Amtrak to develop a formal corrective action plan documenting how Amtrak would address its highest ranked identified vulnerabilities. Additionally, the agency approved Amtrak investment justifications for lower risk vulnerabilities, and did not document roles and responsibilities for the grant project approval process. As a result, some rail stations and the traveling public may be at risk of potential terrorist attack. TSA concurred with our two recommendations and has initiated corrective actions.
(OIG-11-93, June 2011, OA)
http://www.oig.dhs.gov/assets/Mgmt/OIGr_11-93_Jun11.pdf

TSA's Oversight of the Airport Badging Process Needs Improvement
Individuals who pose a threat may obtain airport badges and gain access to secured airport areas. We analyzed vetting data from 359 airport badging offices and identified badge holder records with omissions or inaccuracies pertaining to security threat assessment completions, birth dates, and birthplaces. For example, we identified that badges were issued to individuals without a complete security threat assessment. These problems existed because TSA has designed and implemented only limited oversight of the application process. Consequently, the safety of airport workers, passengers, and aircraft is at risk due to the identified vulnerabilities in the badging process. We made six recommendations to TSA. TSA concurred with five recommendations and partially concurred with one that will improve the effectiveness of safeguards over the badging process.
(OIG-11-95, July 2011, OA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-95_July11.pdf

Transportation Security Administration (TSA) Vetting of Airmen Certificates and General Aviation Airport Access and Security Procedures
We reviewed the actions taken by TSA pursuant to the *Aviation and Transportation Security Act* and the *Intelligence Reform and Terrorism Protection Act of 2004* to determine if individuals who hold a Federal Aviation Administration (FAA) airmen certificate pose a threat to transportation security. As of February 2010, TSA vetted approximately 6.8 million FAA airmen certificates against the Terrorist Screening Database (TSDB), including its subsets, the No Fly and Selectee lists. The TSDB is the U.S. government's consolidated watch list of all known or appropriately suspected terrorists. The results of the vetting process identified about 29,000 certificates that matched names contained in the TSDB. Of those matches, TSA analysts administratively determined that about 28,500 matches were invalid, and TSA analysts did not refer them for a security threat investigation. TSA performed a security threat investigation on the roughly 500 remaining individuals that were determined to be true matches and recommended that 27 airmen certificates be revoked. The report does not contain any recommendations.
(OIG-11-96, July 2011, ISP)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-96_Jul11.pdf

Improvements in Patch and Configuration Management Controls Can Better Protect TSA's Wireless Network and Devices
The use of wireless devices is becoming increasingly popular throughout the federal government; however, its use has also introduced security

threats, all of which may compromise sensitive information. This report identifies measures that TSA can take to enhance the overall security controls and protection of its wireless network and devices. Overall, we determined that TSA has implemented effective physical and logical security controls to protect its wireless network and devices. We did not detect the presence of any rogue or unauthorized wireless networks or devices attributed to TSA or the Federal Air Marshal Service (FAMS). Although we identified signal leakage from TSA's wireless network, we determined that this was not a security risk due to the mitigating controls implemented. However, we identified high-risk vulnerabilities involving TSA's and FAMS's patch and configuration controls. We made four recommendations for improvements needed to enhance the security of wireless components to fully comply with the Department's information security policies and better protect TSA's and FAMS's wireless infrastructure against potential risks, threats, and exploits. TSA management concurred with the recommendations and has already begun to take actions to implement them.
(OIG-11-99, July 2011, ITA)
http://www.oig.dhs.gov/assets/Mgmt/OIGr_11-99_Jul11.pdf

Review of Costs Invoiced by the City of San Francisco Relating to the Terminal 2 Checked Baggage Screening Project at San Francisco International Airport Under Other Transaction Agreement Number HSTS04-09-H-REC123
TSA provided the city of San Francisco $15,346,800 of Recovery Act funds to modify Terminal 2 of the San Francisco International Airport to support installation of a Checked Baggage Inspection System. The funds were provided under Other Transaction Agreement No. HSTS04-09-H-REC123 and represents 90% of estimated eligible project costs of $17,052,000. We audited the city to determine whether costs invoiced under the agreement were allowable, allocable, and reasonable according to the funding agreement and applicable federal requirements. Out of invoiced costs of $12,837,196, we questioned costs of $303,474 for construction management because they were not adequately supported by the accounting records. In addition, TSA needs to review the city of San Francisco's purchases to ensure that the city complied with the requirement to buy American goods.
(OIG-11-104, August 2011, OA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-104_Aug11.pdf

INVESTIGATIONS

TSA Supervisory Transportation Security Officer Sentenced in Connection with $30,000 Theft Scheme
We conducted an investigation into theft allegations involving TSA screener at the Newark Liberty International Airport, Newark, New Jersey. The investigation established that from October 2009 to September 2010, property and currency totaling as much as $30,000 were stolen from passengers as they underwent checkpoint screening. We interviewed a Supervisory Transportation Security Officer (TSO) who admitted stealing currency from passengers' baggage. The Supervisory TSO was sentenced in U.S. District Court to 30 months imprisonment, followed by 36 months supervised release, and ordered to forfeit $24,150.

TSA Employee Guilty of Possessing Child Pornography
In a joint investigation with the U.S. Immigration and Customs Enforcement (ICE) Office of Professional Responsibility, we secured the conviction of a TSO, who was found in possession of child pornography. Agents discovered that the employee, while off duty, routinely used several Internet and social media sites to receive and distribute child pornography. The TSO was initially identified as an employee through a picture he posted on a social media site of him wearing his TSA uniform that he posted on a social media site. The subject is awaiting sentencing.

TSA Employee Pleads Guilty to Stealing from Passenger Luggage
We conducted an investigation into allegations of theft involving a TSO at the Orlando International Airport. The investigation revealed that the TSO stole several laptop computers and other

items from passenger luggage while ostensibly performing his duties at the airport. The employee subsequently pleaded guilty to charges of embezzlement and theft in connection with the investigation.

UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES

MANAGEMENT REPORTS

Information Technology Management Letter for the U.S. Citizenship and Immigration Services Component of the FY 2010 DHS Financial Statement Audit

KPMG LLP, under contract with DHS OIG, conducted the audit of DHS' consolidated balance sheet as of September 30, 2010, and the related statement of custodial activity. KPMG LLP performed an evaluation of ITGC at U.S. Citizenship and Immigration Services (USCIS), to assist in planning and performing the audit. As part of this review, KPMG LLP noted certain matters involving internal control and other operational matters with respect to IT and have documented its comments and recommendation in the Information Technology Management Letter. The overall objective of our audit was to evaluate the effectiveness of IT general controls of USCIS' financial processing environment and related IT infrastructure. KPMG LLP noted that USCIS took corrective action to address many prior years' IT control weaknesses. However, during FY 2010, KPMG LLP continued to find IT general control weaknesses at USCIS. The most significant findings from a financial statement audit perspective were related to the Federal Financial Management System configuration and patch management, and deficiencies within Computer Linked Application Information Management System (CLAIMS) 3 local area network and CLAIMS 4 user account management. Collectively, the IT control deficiencies limited USCIS's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these control deficiencies negatively impacted the internal controls over USCIS financial reporting and its operation, and we consider them to contribute to a material weakness at the Department level under standards established by AICPA.
(OIG-11-74, April 2011, ITA)
http://www.oig.dhs.gov/assets%5CMgmt%5COIG_11-74_Apr11.pdf

U.S. Citizenship and Immigration Services Privacy Stewardship

USCIS is responsible for granting immigration and citizenship benefits, promoting an understanding of citizenship, and ensuring the integrity of our immigration system. Interacting with the public in more than 250 offices around the world, almost 18,000 USCIS employees collect, use, and disseminate personally identifiable information (PII). Our audit objectives were to determine

Stages of Processing Alien Registration Files Containing Personally Identifiable Information
Source: DHS OIG

whether USCIS' plans and activities instill a culture of privacy and whether USCIS complies with federal privacy laws and regulations.

USCIS demonstrated an organizational commitment to privacy stewardship by appointing a privacy officer and establishing its Office of Privacy. The Office of Privacy monitors compliance with federal privacy laws and regulations and provides guidance to managers and employees on meeting requirements for notice, incident reporting, and privacy impact assessments. In addition, the Office of Privacy conducts initial and annual privacy training and addresses inquiries and complaints by individuals.

While USCIS has made progress in implementing a privacy program that complies with privacy laws, opportunities still exist to improve its privacy culture. USCIS can strengthen its privacy culture by improving administrative, physical, and technical safeguards that protect PII.
(OIG-11-85, May 2011, ITA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-85_May11.pdf

The U.S. Citizenship and Immigration Services' Adjudication of Petitions for Nonimmigrant Workers (I-129 Petitions for H-1B and H-2B visas)
USCIS responsibilities include collecting, processing, and adjudicating visa petitions submitted by employers seeking permission to temporarily employ foreigners as nonimmigrant workers in the United States. Employers use Form I-129 (Petition for Nonimmigrant Worker) to request permission to bring foreign individuals to the United States temporarily to perform services or labor, or to receive training under the H-1B and H-2B visa classifications. Immigration Services Officers (ISOs) are the first to review I-129 petitions for H-1B or H-2B visas.

Our review determined that the ISO fraud training for the adjudication of the H-1B and H-2B visa classifications of the I-129 petitions is decentralized and inconsistent. Although USCIS has a process to train newly hired ISOs, fraud training varies, and ongoing fraud training is not updated and provided annually. Our two recommendations called for USCIS to develop and implement a national, post-basic fraud identification and response training program that identifies current fraud trends; and ensure that this fraud training is conducted annually for all ISOs and supervisors responsible for H-1B and H-2B adjudications. USCIS concurred with both recommendations.
(OIG-11-105, August 2011, OA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-105_Aug11.pdf

INVESTIGATIONS

Certificates of Naturalization Canceled Due to Fraud
As part of our continuing investigation related to the case of a former USCIS Supervisory Adjudication Officer (AO) in which numerous aliens fraudulently obtained immigration benefits, the DHS OIG arrested two additional civilian conspirators. One subject who had illegally obtained genuine immigration documents in exchange for cash payments pleaded guilty to Procuring Citizenship Unlawfully. The subject was sentenced on July 1, 2011, to 3 years probation, $100 assessment, and cancellation of all naturalization documents. A similar offender pleaded guilty to Fraud Involving Computers. The subject was sentenced to 3 years supervised probation, $125 assessment, and cancellation of all naturalization documents.

Department of Defense Contract Employee Pleads Guilty to Immigration Fraud
We arrested a Department of Defense (DOD) contract employee who had secured a Top Secret security clearance using his fraudulently obtained immigration status. Our prior arrest of a USCIS Supervisor led to information concerning hundreds of aliens who fraudulently obtained immigration benefits by paying bribes to the USCIS employee. On July 7, 2011, the DOD contract employee pleaded guilty to Immigration Fraud and is awaiting sentencing.

USCIS District Adjudications Officer Pleads Guilty to Accepting Bribes
We investigated a USCIS District AO, Garden City, New York, for soliciting and accepting bribes in exchange for favorable treatment in processing citizenship applications of permanent resident aliens. During the course of the naturalization interviews, the AO demanded bribes from applicants to approve their paperwork. The AO would then meet with the applicants near their homes to collect the money. The officer pleaded guilty to one count of Bribery and is awaiting sentencing.

Foreign Exchange Students Victims of Fraud
We investigated a subject who was defrauding prospective foreign exchange students by fraudulently claiming to have a connection to a USCIS employee who could facilitate the approvals of foreign exchange student applications. The subject, a non-DHS employee, charged each student $6,000 for the fraudulent application process. The subject pleaded guilty to wire fraud and is awaiting sentencing.

Supervisory Immigration Services Officer (ISO) and Son Sentenced for Accepting Bribes
We participated in a joint investigation with ICE Homeland Security Investigations concerning a USCIS Supervisory ISO and his 46-year-old, non-DHS employee son who accepted money from a confidential informant in exchange for checking the status of USCIS applications and collected money from immigration applicants in exchange for the issuance of USCIS benefits. On August 11, 2011, the Supervisory ISO (who retired in January 2010) was sentenced to 60 months confinement, 36 months supervised release, and ordered to pay a fine of $30,000. The ISO's son was sentenced to 48 months confinement and 60 months supervised release.

UNITED STATES COAST GUARD

MANAGEMENT REPORTS

Information Technology Management Letter for the United States Coast Guard Component of the FY 2010 DHS Financial Statement Audit
KPMG LLP, under contract with DHS OIG, conducted the audit of United States Coast Guard (USCG) consolidated balance sheet in support of DHS' financial statement audit as of September 30, 2010. As part of this review, KPMG LLP noted certain matters involving internal control and other operational matters with respect to IT and documented its comments and recommendation in the Information Technology Management Letter. The overall objective of our audit was to evaluate the effectiveness of IT general controls of USCG's financial processing environment and related IT infrastructure. KPMG LLP noted that USCG took corrective action to address many prior years' IT control weaknesses. However, during FY 2010, KPMG LLP continued to find IT general control weaknesses at USCG. The most significant weaknesses from a financial statement audit perspective are related to control over authorization, development, implementation, and tracking of IT scripts at the Finance Center. Collectively, the IT control weaknesses limit USCG's ability to ensure that critical financial and operational data are maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively impact the internal controls over USCG's financial reporting and its operation, and KPMG LLP considers them to collectively represent a material weakness at the Department level under standards established by AICPA.
(OIG-11-80, May 2011, ITA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-80_May11.pdf

U.S. Coast Guard's Anti-Deficiency Act Violations for the Response Boat-Medium Major Acquisition Project for Fiscal Years 2004 Through 2009

We conducted an audit to determine whether *Anti-Deficiency Act* (ADA) violations occurred through improper use of appropriations during the administration of the Response Boat-Medium Major Acquisition project between fiscal years 2004 and 2009. We determined that USCG exceeded its appropriated funding for the Response Boat-Medium project during fiscal years 2004 through 2009. We recommended that USCG notify the Secretary that it incurred 20 ADA violations totaling approximately $7 million and identify the names of the responsible parties. We also recommended that USCG revise its standard operating procedures for future acquisitions. USCG concurred with both recommendations and has taken correction action to address them. (OIG-11-82, May 2011, OA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-82_May11.pdf

USCG's Response Boat-Medium.
Source: USCG Photo library

USCG's 41-foot Utility Boat.
Source: USCG Photo Library

U.S. Coast Guard's Marine Safety Program – Offshore Vessel Inspections

We planned this audit to determine whether USCG's Marine Safety program has the capabilities and resources needed to inspect offshore vessels. We determined that USCG does not have adequate information to plan and resource future Marine Safety program activity levels. The Marine Safety program has not developed and implemented all guidance needed by Marine Inspectors to conduct offshore vessel inspections and record the results of those inspections. Program officials also have not established a formal review process for Marine Safety domestic vessel inspection data. These gaps in guidance may affect the quality and consistency of safety inspections. Without a formal policy and procedure in place requiring the review of inspection data, program personnel could be using inconsistent and unreliable inspection data and do not have the capability to make accurate program decisions. We made four recommendations to USCG, including developing and implementing needed guidance for Marine Inspectors and establishing certain controls over inspection data. USCG concurred with all four recommendations and submitted a corrective action plan and a projected completion date for each recommendation. (OIG-11-86, June 2011, OA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-86_Jun11.pdf

Coast Guard Has Taken Steps to Strengthen Information Technology Management, but Challenges Remain

We audited USCG's management of IT. The objective of our audit was to determine the effectiveness of USCG's planning, acquisition, implementation, and use of technology to support its mission. USCG has made progress establishing effective IT management practices. As a result,

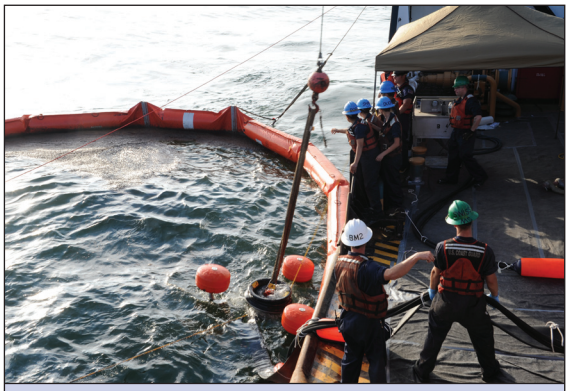
the CIO is positioned to support the USCG's mission of marine safety, security, and stewardship, and has controls in place to allow for effective acquisition decisions. The CIO has also taken steps to centralize and standardize implementation of IT across USCG. Achieving a standard IT environment, however, has been hampered by the CIO's limited authority over some IT assets and spending. Consequently, the CIO cannot fully ensure that the IT environment is functioning effectively and efficiently. USCG could improve IT management in a number of areas. Specifically, USCG systems and infrastructure do not fully meet mission needs. We made six recommendations to USCG and include completing the transition of IT personnel and oversight of field IT spending under the CIO. These recommendations focus on planning and implementing requirements that will enhance specific IT assets and their capabilities. The CIO concurred with the recommendations and provided information on how USCG is already working to address the recommendations.
(OIG-11-108, September 2011, ITA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-108_Sep11.pdf

Annual Review of the United States Coast Guard's Mission Performance (FY 2010)
The Homeland Security Act of 2002 requires DHS OIG to conduct an annual review of USCG's mission performance. We reviewed USCG's performance measures and results for each non-homeland security and homeland security mission, as well as resource hours used to perform the various missions from fiscal years 2001 through 2010. We determined that USCG dedicated about the same hours to non-homeland security missions as to homeland security missions. However, this parity was not by design but rather due to several major events, including the Deepwater Horizon oil spill in the Gulf of Mexico and Haiti earthquake relief efforts. USCG met more non-homeland security performance measures than homeland security performance measures. USCG's budget information for fiscal year 2011 and projections for fiscal year 2012 show a slight increase in homeland security mission spending and a slight decrease in non-homeland security spending from fiscal year 2010. USCG agreed with our analysis. The report contained no recommendations.
(OIG-11-111, September 2011, OA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-111_Sep11.pdf

United States Coast Guard's Internal Controls and Cost Capturing for the Deepwater Horizon Oil Spill
We planned this audit to determine whether USCG has adequate policies, procedures, and internal controls to accurately capture direct and indirect costs for the Deepwater Horizon oil spill. We determined that USCG has adequate policies, procedures, and internal controls to accurately identify and bill direct costs for this oil spill.

Fireboat response crews battle the blazing remnants of the offshore oil rig Deepwater Horizon on April 21, 2010.
Source: USCG Photo library

A USCG crewmember monitors a hose transporting an oil-and-water mix from the Spilled Oil Recovery System.
Source: USCG Photo library



Oil is collected in skimming boom.
Source: USCG Photo Library

USCG recovers oil in the Gulf of Mexico less then one mile from the shoreline June 20, 2010.
Source: USCG Photo Library

USCG aircrew members, from a C-130 aircraft stationed at USCG Air Station Clearwater, Florida, prepare to drop a satellite-enabled data marker buoy into the Gulf of Mexico to help track the spill on May 29, 2010.
Source: USCG Photo Library

However, the unprecedented size of this oil spill revealed weaknesses in USCG's existing processes for capturing indirect costs. As a result, USCG may not be able to bill for as much as $193.7 million in indirect costs. Additionally, USCG cannot bill as much as $38.7 million because its standard reimbursable rates instruction was not updated as scheduled, which would have been prior to the oil spill. USCG took immediate corrective action on issues identified during our audit. We made three recommendations for USCG to improve internal controls, processes, and systems to accurately capture and bill all allowable costs associated with this oil spill and future oil spills; USCG concurred with the three recommendations.
(OIG-11-115, September 2011, OA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-115_Sep11.pdf

INVESTIGATION

USCG Auxiliary Member Used Government Credit Cards to Purchase Cocaine

In a joint investigation with USCG Investigative Service and General Services Administration, our agents determined that a member of the USCG Auxiliary used government fleet credit cards to purchase gasoline for a narcotics dealer in exchange for cocaine. The investigation also discovered that the auxiliary employee used government fleet cards to purchase gasoline for himself, his friends, and family. He ultimately admitted his guilt and was allowed to participate in a pretrial diversion program. He was also ordered to serve 12 months of unsupervised release and ordered to pay $8,000 in restitution.

UNITED STATES CUSTOMS AND BORDER PROTECTION

MANAGEMENT REPORTS

Information Technology Management Letter for the FY 2010 U.S. Customs and Border Protection Financial Statement Audit

KPMG LLP, under contract with DHS OIG, conducted the audit of Customs and Border Protection (CBP) Consolidated Financial Statements as of September 30, 2010. As part of this review, KPMG LLP noted certain matters involving internal control and other operational matters with respect to IT and have documented its comments and recommendation in the IT management letter. The overall objective of our audit was to evaluate the effectiveness of IT general controls of CBP's financial processing environment and related IT infrastructure. KPMG LLP noted that CBP took corrective action to address many prior years' IT control weaknesses. However, during FY 2010, KPMG LLP continued to find IT general control weaknesses at CBP. The most significant weaknesses from a financial statement audit perspective related to access controls, and service continuity. Collectively, the IT control weaknesses limit CBP's ability to ensure that critical financial and operational data are maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively impact the internal controls over CBP's financial reporting and its operation, and KPMG LLP considers them to collectively represent a significant deficiency under standards established by AICPA.
(OIG-11-90, June 2011, ITA)
http://www.oig.dhs.gov/assets/Mgmt/OIGr_11-90_Jun11.pdf

Efficacy of Customs and Border Protection's Bonding Process

Our objective was to determine the efficacy of CBP's process for determining and applying bonds in sufficient amounts to cover importer duties, fees, and taxes. Although CBP has strong controls over continuous bonds, it lacks adequate controls over the single transaction bond process, and its method for determining and applying single transaction bonds is ineffective. We estimate that approximately $8 billion of $12 billion in single transaction bonds accepted by CBP during FY 2009 contain errors that may result in noncollection. Additionally, our results show $1.5 billion at risk of loss for imports subject to other government agency requirements. We made four recommendations to assist CBP in improving program performance. CBP officials concurred with all the recommendations.
(OIG-11-92, June 2011, OA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-92_Jun11.pdf

Use of American Recovery and Reinvestment Act Funds by U.S. Customs and Border Protection for Construction of Land Ports of Entry

We performed an audit to determine whether CBP's approach to constructing land ports of entry on the northern border with *American Recovery and Reinvestment Act* (Recovery Act) funds was reasonable. The Recovery Act provided CBP with $420 million for improving 43 CBP-owned ports. CBP is reconstructing 30 northern border ports with the Recovery Act funds. CBP developed reasonable plans, including the use of three standard port designs ranging in overall size from approximately 4,300 to 10,000 square feet. However, some of the features in the standard designs are not supported by operational requirements, and the basis for the port design selected for certain locations is not adequately supported. Furthermore, CBP is building three new ports and repairing one port that its field offices recommended be closed instead of being improved with Recovery Act funds. We recommend that the agency reevaluate its design selections for five ports and modernization approach for five other ports that it ranked high for potential closure and determine whether they should be repaired, rebuilt, or closed.
(OIG-11-97, July 2011, OA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-97_Aug11.pdf

Security Issues with U.S. Customs and Border Protection's Enterprise Wireless Infrastructure

Wireless networks and devices present significant security challenges. This includes risks due to

weak technical and physical controls of wireless devices or the installation of unauthorized wireless network devices. This report identified measures that CBP should take to further improve the effectiveness in securing its Enterprise Wireless Infrastructure (EWI).

CBP has made progress in improving the EWI security controls by publishing wireless policy and implementation guidance; certifying and accrediting EWI; performing an independent security test and evaluation that identified security program risks; establishing adequate technical security configurations to protect EWI against commonly known security vulnerabilities; and incorporating wireless security awareness into its annual rules of behavior employee training.

Despite these efforts, additional steps are needed to further strengthen EWI. CBP needs to (1) manage and remediate the deficiencies indentified in the EWI plan of action and milestones to ensure that corrective actions are taken, (2) enable wireless intrusion detection functionality to monitor network activity that is incorporated into EWI's hardware devices, and (3) perform regular vulnerability assessments to ensure that wireless networks and devices are operating securely. We made three recommendations that, if implemented, could improve the EWI security posture. CBP management concurred with the recommendations and has begun to take corrective actions to implement them.
(OIG-11-118, September 2011, ITA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-118_Sep11.pdf

INVESTIGATIONS

CBP Officer Sentenced for Accepting Bribes from Drug Traffickers
A CBP Officer assigned to the port of entry (POE) in Pharr, Texas, was sentenced to 24 months probation in connection with a scheme to facilitate the smuggling of marijuana into the United States. Our investigation revealed that the CBP Officer accepted $10,000 in bribes to allow vehicles laden with marijuana to enter the United States through his primary inspection lane. The investigation resulted in the CBP Officer being convicted of Acts Affecting a Personal Financial Interest.

CBP Officer Admits to Acting as a Lookout for Drug Traffickers
During the investigation of a murder in Stockholm, New York, it was determined that a CBP Officer from Massena, New York, was associated with the murder victim, who was reportedly involved in narcotics trafficking. During questioning, the CBP Officer admitted to acting as a "lookout" for the murder victim during transport of marijuana from northern New York to Cleveland, Ohio. The CBP Officer also transported marijuana proceeds from Cleveland, Ohio to northern New York on the murder victim's behalf. The CBP Officer received approximately $15,000 for his part in the drug transactions. The CBP Officer pleaded guilty to one count of manufacture, distribution, and possession of narcotics, resigned from CBP, and is awaiting sentencing.

CBP Officer Conspired with Transnational Drug Traffickers
We developed information that a CBP Officer used his position at the Hartsfield-Jackson International Airport, Atlanta, Georgia, to support international drug trafficking organizations. We began a multi-agency Organized Crime Drug Enforcement Task Force investigation leading to the suppression of the drug trafficking organizations and arrest of multiple offenders. Our investigation revealed that on 19 separate occasions, the CBP Officer bypassed security, using his own issued airport security badge, in order to smuggle money and weapons. The CBP Officer was convicted and sentenced to serve 8 years of incarceration for money laundering, bulk cash smuggling, entering an aircraft area in violation of security procedures, carrying a weapon on an aircraft, fraud and related activity in connection with computers, and conspiracy to commit marriage fraud.

CBP Officer Pleaded Guilty to Visa Fraud
A CBP Officer assigned to Detroit, MI, pleaded guilty in the U.S. District Court for the Eastern District of Tennessee to falsely altering an

immigration document. Our investigation determined that the CBP Officer exceeded her authority by fraudulently changing the status of two nonimmigrant visa holders. The officer subsequently admitted to fraudulently adjusting the status of the dependent of an Iranian citizen who was studying at a local university.

Border Patrol Agent (BPA) Pleads Guilty to Assaulting a Fellow BPA

We investigated an allegation that a BPA assigned to Wilcox, Arizona, assaulted a fellow BPA while on duty by threatening him with a loaded firearm. The investigation resulted in the conviction of the BPA on charges of assaulting a federal officer. The BPA was sentenced to time served and ultimately was dismissed from the Border Patrol.

Border Patrol Agent Harbored Undocumented Mexican National

A BPA working in southeast Texas was sentenced to 3 years probation as a result of our investigation into allegations that he harbored an undocumented Mexican national. During the investigation, agents observed the BPA and his illegal alien ex-wife attempt to enter the U.S. through a POE. The BPA was detained but declined to cooperate. His spouse provided agents with a sworn statement acknowledging her status as an undocumented alien. A search warrant executed at the BPA's residence found evidence of his cohabitation with the undocumented former spouse, a fraudulent Social Security card and, a fraudulently obtained U.S. birth certificate in the former spouse's name.

CBP Officer Convicted in Alien Smuggling Scheme

Our investigation resulted in the conviction of an El Paso, Texas CBP Officer for smuggling undocumented aliens into the United States. The employee was proven to have conspired with a non-DHS employee to facilitate the illegal crossing of undocumented aliens through his assigned inspection lane, for a fee of $5,000. The CBP Officer's co-conspirator was convicted and sentenced for participating in the scheme. He was sentenced to serve 27 months of incarceration and 3 years of supervised release.

UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT

MANAGEMENT REPORTS

Information Technology Management Letter for the Immigration and Customs Enforcement Component of the FY 2010 DHS Financial Statement Audit

KPMG LLP, under contract with DHS OIG, conducted the audit of DHS' consolidated balance sheet as of September 30, 2010, and the related statement of custodial activity. KPMG LLP performed an evaluation of ITGC at ICE, to assist in planning and performing the audit. As part of this review, KPMG LLP noted certain matters involving internal control and other operational matters with respect to IT and have documented its comments and recommendation in the Information Technology Management Letter. The overall objective of our audit was to evaluate the effectiveness of IT general controls of ICE's financial processing environment and related IT infrastructure. KPMG LLP noted that ICE took corrective action to address many prior years' IT control weaknesses. However, during FY 2010, KPMG LLP continued to find IT general control weaknesses at ICE. The most significant weaknesses from a financial statement audit perspective related to controls over the Federal Financial Management System and weaknesses in physical security and security awareness. Collectively, the IT control weaknesses limit ICE's ability to ensure that critical financial and operational data are maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively impact the internal controls over ICE's financial reporting and its operation, and KPMG LLP considers them to collectively represent a material weakness under standards established by AICPA.
(OIG-11-70, April 2011, ITA)
http://www.oig.dhs.gov/assets%5CMgmt%5COIG_11-70_Apr11.pdf

Supervision of Aliens Commensurate with Risk
ICE is responsible for detaining and removing deportable aliens from the United States. On September 30, 2009, ICE had more than 1.6 million active alien cases classified as either detained or non-detained. Detained aliens are those held in ICE detention facilities, while non-detained aliens include incarcerated criminal aliens and aliens released on supervision. We assessed the effectiveness of ICE's decision making process on whether to detain aliens in an ICE facility or place them in supervised release. ICE generally has an effective decision making process for determining whether to detain or release aliens. However, personnel could not always provide evidence that aliens were screened against the Terrorist Watchlist. Policy for screening aliens from designated countries is not effective; and personnel did not always maintain accurate and up-to-date information in the case management system. Our report includes three recommendations for ICE to (1): enforce current policy and procedures for screening aliens against the Terrorist Watchlist; (2) revise ICE's current policy to require officers to conduct Third Agency Checks for all aliens from specially designated countries; and (3) develop procedures to ensure that officers comply with requirements to maintain accurate information. ICE concurred with recommendation #1 and #3. Based on ICE's corrective action plan, we consider these recommendations resolved. ICE did not concur with recommendation #2, and we consider this recommendation unresolved. (OIG-11-81, May 2011, OA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-81_May11.pdf

DHS Detainee Removals and Reliance on Assurances
The Special Interagency Task Force on Interrogation and Transfer Policies requested that the Inspectors General from DHS, State, and Defense report on the removals conducted by each agency in reliance on diplomatic assurances of humane treatment of persons transferred to another country. In the immigration context, diplomatic assurances are written documents or communications from a foreign country designed to reduce the risk of torture to an individual if removed to that country. Specifically, the Task Force requested that the three Departments report on the process for obtaining assurances, their content, and implementation, as well as the post-removal treatment of persons transferred between August 24, 2009, and August 25, 2010, when removals involved obtaining assurances.

DHS did not seek or obtain assurances during the reporting period. Nevertheless, we sought to understand DHS' role in obtaining and validating assurances and monitoring post-removal treatment in the immigration context, in compliance with Article 3 of the United Nations Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT), as implemented in U.S. law.

Although we did not make any recommendations, there are aspects of the assurances process that warranted examination. For example, the regulations are silent as to potential candidates for assurances, factors countries may consider when contemplating a candidate, and the content of assurances. Furthermore, though the Convention and the legislation implementing U.S. treaty obligations under the Convention do not define reliability regarding assurances, Department officials, a Department of State official, and NGO representatives discussed with us factors to consider when assessing reliability. There appears to be a consensus within DHS that assurances need to be fact-specific, and someone with protection expertise should be involved in determining reliability factors consistent with those recommended by the Task Force. (OIG-11-100, July 2011, ISP)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-100_Jul11.pdf

The Performance of 287(g) Agreements FY 2011 Update
Section 287(g) of the *Immigration and Nationality Act*, as amended, authorizes DHS to delegate federal immigration enforcement authorities to state and local law enforcement agencies through formal, written agreements. The agreements outline terms and conditions for program activities and establish a process for ICE to supervise and

manage program functions. This report is an update to two OIG reports, 1) OIG-10-63, *The Performance of 287(g) Agreements*, issued in March 2010 and 2) OIG-10-124, *The Performance of 287(g) Agreements Report Update*, issued September 2010, with a total of 49 recommendations to improve overall operations of the 287(g) program.

In this review, we determined that ICE needs to continue efforts to implement our prior recommendations. In addition, we identified challenges that may reduce the effectiveness of a review process intended as a resource for ensuring compliance with 287(g) program requirements. We recommended that ICE: (1) provide training to inspectors to ensure that they have sufficient knowledge of the 287(g) program and the Memorandum of Agreement with state and local law enforcement agencies, and other skills needed to conduct effective inspection reviews; (2) develop and implement comprehensive analytical tools for use as part of the inspection review process: and (3) review and revise the Memorandum of Agreement with participating law enforcement agencies to ensure a clear understand of 287(g) program requirements. We made 13 recommendations for ICE to improve overall operations of the 287(g) program.
(OIG-11-119, September 2011, ISP)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-119_Sep11.pdf

INVESTIGATIONS

DHS Contract Correctional Officer Sentenced to 10 Months in Prison
We investigated an allegation against a contract Correctional Officer (CO) at an ICE detention facility involving sexual abuse of a federal immigration detainee. We interviewed the CO, who admitted to coerced sexual contact with the detainee, a Mexican citizen. The CO pleaded guilty to sexual abuse of a ward of the government and was sentenced in the U.S. District Court for the Western District of Louisiana to 10 months incarceration.

Bribe Attempt by Detainees Ends in Arrests and Guilty Pleas
We investigated an allegation from an ICE Detention and Removal Assistant (DRA) who was approached by detainees who were on bond awaiting an immigration hearing. The detainees attempted to bribe the DRA with money in exchange for leniency in the mandated reporting process to ICE Enforcement and Removal. Three detainees pleaded guilty to bribing a public official and are awaiting sentencing.

Individual Sentenced to 72 Months for $130,000 Immigration Fraud Scheme
We investigated a private citizen who was alleged to be impersonating an immigration official in order to defraud prospective immigrants. According to the information received, the complainant and her daughter made cash payments to the subject in order to not be reported to DHS and were threatened with deportation if they refused to pay. Our investigation determined that the subject received in excess of $130,000 in cash payments as the result of his scheme. The subject was subsequently convicted of impersonating a federal officer and wire fraud. He was sentenced to serve 72 months confinement and ordered to pay $100,000 in restitution.

ICE Detention Officer Uses Stolen Admissions Stamp in Visa Fraud Scheme (Update from 10/01/10-03/31/11 Semiannual Report to the Congress)
A former Detention and Removal Officer (DRO) was sentenced to 46 months in federal prison for taking bribes totaling at least $28,500 to allow foreign employees (and their spouses) of now-closed restaurants in Chicago, Illinois and nearby Downers Grove to extend their stays in the United States. Our investigation determined that the DRO received approximately $1,500 from at least 19 restaurant employees and their spouses to alter a law enforcement database and provide false immigration and travel documents showing that the restaurant workers and their spouses had just entered the United States and were eligible to legally stay in the country for another year.

Bribery of ICE Official Leads to Arrest of Co-Conspirator

We investigated an allegation that an ICE Special Agent who allegedly facilitated an inordinately high amount of alien paroles, had a large amount of contact with defense attorneys, a high level of personal foreign travel, and had allegedly been involved in international transportation of gold. The investigation determined that an individual had delivered approximately $109,000 to an ICE Special Agent. The individual was charged with Bribery of a Public Official, was convicted and is awaiting sentencing. The ICE Special Agent has not been charged.

MULTIPLE COMPONENTS

MANAGEMENT REPORTS

Information Sharing On Foreign Nationals: Overseas Screening

The December 25, 2010, terrorist attempt to bomb an airline flight from Amsterdam to Detroit highlighted the importance of information sharing between the components of DHS. We reviewed programs DHS has implemented to screen foreign national travelers while they are still overseas, including levels of cooperation, resources, and technology. We also reviewed plans to improve DHS data systems. We concluded that the level of cooperation among components that conduct overseas screening is high, and that DHS has made progress in evaluating admissibility of foreign nationals before they travel to the United States. However, we concluded that DHS faces serious resource and technological challenges, uses data systems that are fragmented and difficult to use, and requires additional staffing and resources for some important screening programs. We made 18 recommendations to standardize the technology used to share information in DHS data systems, enable federal officers to obtain and use the most current and complete data available, and improve information sharing procedures. DHS components concurred with 17 of the recommendations, but they report that they currently do not have the resources to implement 5 of the recommendations with which they concurred. (OIG-11-68, April 2011, ISP)
http://www.oig.dhs.gov/assets/mgmt/OIGr_11-68_Apr11.pdf

Special Report: Summary of Significant Investigations, October 1, 2009, to December 31, 2010

Congress enacted the *Inspector General Act of 1978*, as amended, to ensure integrity and efficiency in government operations and activities. The *Homeland Security Act of 2002*, as amended, established an OIG in DHS. Under these authorities, the OIG serves as an independent and objective audit, inspection, and investigative body to promote effectiveness, efficiency, and economy in the Department's programs and operations, and to prevent and detect fraud, abuse, mismanagement, and waste in such programs and operations.

As part of our oversight responsibilities, the Office of Investigations prepared this special report that focused on our investigative efforts over the 15-month period, from October 1, 2009, through December 31, 2010. We provided narrative descriptions of significant investigations conducted independently by our Office of Investigations, as well as in cooperation with other partnering law enforcement agencies. We cited investigative work which involved the operations and activities of the relevant DHS components as listed herein: FEMA, FPS, TSA, USCG, CBP, USCIS, ICE, and the U.S. Secret Service (USSS).

This special report contributed significantly to the Department's overall mission, and specifically addressed the Secretary's priorities and goals concerning (1) Preventing Terrorism and Enhancing Security and (2) Securing and Managing the Nation's Borders. Our work was based on interviews with employees and officials of relevant agencies and institutions, direct observations, and review of applicable documents. (OIG-11-72, April 2011, INV)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-72_Apr11.pdf

DHS/U.S. Secret Service FY 2009 Antideficiency Act Violation

To cover a shortfall in its 2008 presidential candidate protection budget, USSS obligated funds more than 10% in excess of its FY 2009 appropriation prior to submitting a reprogramming request to DHS. DHS was required to notify Congress 10 days prior to the reprogramming. As a result, the funds USSS obligated in excess of its appropriations were not legally available. GAO reported that DHS and USSS violated ADA, which prohibits the obligation of funds in excess of available appropriations. In conducting a follow-up review, we determined that USSS' former CFO was responsible for the FY 2009 ADA violation. However, we found no evidence that the former CFO acted with knowledge or willful intent to violate the law. We recommended that the DHS Under Secretary for Management comply with ADA reporting requirements, ensure that DHS and USSS implement the joint corrective action plan, and implement the recommendations previously issued by GAO. The DHS Under Secretary for Management concurred with each of our recommendations.
(OIG-11-94, July 2011, OA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-94_Jul11.pdf

Evaluation of DHS' Security Program and Practices for Intelligence Systems for Fiscal Year 2011

We reviewed DHS' enterprise-wide security program and practices for Top Secret/Sensitive Compartmented Information intelligence systems. Pursuant to the *Federal Information Security Management Act of 2002*, we reviewed the Department's security management, implementation, and evaluation of its intelligence activities, including its policies, procedures, and system security controls for enterprise-wide intelligence systems. The Department continued to improve its information security management program for intelligence systems. DHS has developed information security policies and procedures and implemented effective security controls on intelligence systems. While system controls have been strengthened, more oversight is needed to ensure that the security program's policies are implemented. We have concerns with the oversight of component plans of actions and milestones, verification of the intelligence systems inventory, establishment of a Department-wide continuous monitoring program, and development of an information security training program for intelligence personnel. Our report to the Inspector General of the Office of the Director of National Intelligence did not contain any recommendations.
(OIG-11-98, July 2011, ITA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-98_Jul11.pdf

DHS' Role in Nominating Individuals for Inclusion on the Government Watchlist and Its Efforts to Support Watchlist Maintenance

Although the Department is predominantly a consumer of watchlist information, all seven components contribute to nominating individuals and to enhancing and maintaining watchlist information. The Department, however, recently established a Watchlisting Cell to serve as the central coordination point for all Department nomination and maintenance efforts. As the cell further refines its operational capabilities, it is necessary to develop guidance, provide advanced analysis, and ensure that Departmental efforts do not contradict current component interactions with federal watchlisting entities. The Watchlisting Cell has demonstrated value and is streamlining processes in collaboration with Department components. The Department's most significant contribution to the watchlisting community is the collection and analysis of encounter packages. This information is critical to enhancing existing database records; however, quality and legibility issues exist with how this information is currently collected. The Watchlisting Cell should ensure that its resources are sufficient to provide relevant, accurate, and timely information to internal and external watchlisting partners. We made 10 recommendations to improve the Department's contributions to the federal government's watchlisting process. DHS concurred with all recommendations.
(OIG-11-107, September 2011, ISP)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-107_Sep11.pdf

Review of the Department of Homeland Security's Capability to Share Cyber Threat Information
DHS has taken actions to create an environment to promote cyber threat information sharing in support of its mission. Specifically, DHS has developed an internal-external communication plan to strengthen the partnership between the federal agencies and the private sectors.

We recommended that the Department improve its cyber threat information sharing by strengthening its public-private partnership to ensure better communication with government and sector coordinating councils and the private sector's Information Sharing and Analysis Centers. Also DHS must delineate the roles and responsibilities between the National Cybersecurity and Communication Integration Center and the United States Computer Emergency Readiness Team to avoid confusion among federal agencies and the private sector. Finally, granting DHS the enforcement authority to compel agencies to implement its recommended corrective action recommendations can help to mitigate security incidents.
(OIG-11-117, September 2011, ITA)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-117_Sep11.pdf

INVESTIGATION

Security Specialist Involved in Contract Rigging Scheme
A DHS Physical Security Specialist pleaded guilty to improperly providing internal DHS documents to a government contract company. Our investigation revealed that the employee had received approximately $200,000 from the contractor during a 2-year period. The employee was sentenced to 12 months probation and barred from future employment with the federal government.

OTHER OFFICE OF INSPECTOR GENERAL ACTIVITIES

OVERSIGHT OF NONDEPARTMENTAL AUDITS

During this period, DHS OIG did not process any single audit reports issued by other independent public accountant organizations. Single audit reports refer to audits conducted according to the *Single Audit Act of 1996*, as amended by P.L. 104-136.

DHS will: (1) monitor and identify improvements to DHS' policies and procedures governing its grants management programs; (2) use the results of audits and investigations of grantees and subgrantees as a tool for identifying areas for further analysis, and for helping DHS improve grants management practices and program performance; (3) support DHS in its efforts to monitor and follow up on recommendations from independent external audits of DHS' grantees and subgrantees under the *Single Audit Act*, as amended; (4) perform quality reviews of independent auditors to assure consistency and adherence to Single Audit guidelines.

COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY (CIGIE) REPORTS

Compendium of Disaster Preparedness Programs
In April 2009, DHS OIG issued the *Compendium of Disaster Assistance Programs* (OIG-09-49), an inventory of programs across the federal government that provide assistance after a disaster. The *Compendium of Disaster Preparedness Programs* is a companion document that includes an inventory of federal programs that provide disaster preparedness assistance to individuals, states, localities, nonprofit organizations, businesses, and other public entities. It is based on a survey of members of the CIGIE and a review of the General Services Administration's *Catalog of Federal Domestic Assistance*. The compendium is intended to provide a comprehensive resource of federal disaster preparedness programs.
(OIG-11-88, June 2011, EMO)
http://www.oig.dhs.gov/assets/Mgmt/OIG_11-88_Jun11.pdf

Recommended Practices for Office of Inspectors General Use of New Media
In the fall of 2010, the CIGIE Homeland Security Roundtable asked the DHS Inspector General to lead a working group to explore new media use among OIGs. CIGIE sought to create a forum for OIGs to discuss how they can use new media, as well as how they can oversee their agencies' use of new media. Fifteen OIGs were represented on the CIGIE New Media Working Group. Our charter called for members to explore how OIGs could use new media to serve the OIG mission, research legal and information security issues, and discuss recommended practices. We administered a survey of OIG new media use among 79 CIGIE members to seek input on areas such as the reasons why OIGs are using new media, the tools they are using or considering, overall experiences, resources expended, oversight issues, obstacles, metrics, and legal and information security requirements. Final responses were received from 39 OIGs, two-thirds of which identified themselves as new media users. The report contains six recommendations to facilitate OIGs' effective use of new media.
(OIG-11-120, September 2011, OC)
http://www.oig.dhs.gov/assets/mgmt/OIG_11-120_Sep11.pdf

Management Advisory Report On Cybersecurity
The community of Inspectors General must be proactive in preventing and addressing issues relating to cybersecurity, both in its oversight capacity and in its operational role. To that end, the CIGIE Cybersecurity Working Group was charged with identifying measures that the Inspector General community can take to protect itself against cyber attacks. This report covers four areas identified as cybersecurity challenges facing the Inspectors General community: (1) asset management and leveraging resources; (2) identity, credential, and access management; (3) incident detection and handling; and (4) scalable trustworthy systems.

The report offers recommended practices for the Inspectors General community taking into consideration the different risks or vulnerabilities of each OIG based on the degree to which information technology systems are dependent upon or connected to their parent agencies and whether they have sufficient human and financial resources to secure their information technology systems effectively.
(OIG-11-121, September 2011, ITA)
http://www.oig.dhs.gov/assets/mgmt/OIG_11-121_Sep11.pdf

SUMMARY OF SIGNIFICANT REPORTS UNRESOLVED OVER 6 MONTHS

Timely resolution of outstanding audit recommendations continues to be a priority for both our office and the Department. As of this report date, we are responsible for monitoring 173 reports containing 691 recommendations that have been unresolved for more than 6 months.

93	FEMA-related financial assistance disaster audits
80	Program management reports
173	**Total**

LEGISLATIVE AND REGULATORY REVIEWS

Section 4(a) of the *Inspector General Act* requires the Inspector General to review existing and proposed legislation and regulations relating to DHS programs and operations and to make recommendations about their potential impact. Our comments and recommendations focus on the effect of the proposed legislation and regulations on economy and efficiency in administering DHS programs and operations or on the prevention and detection of fraud, waste, and abuse in DHS programs and operations. We also participate on the CIGIE, which provides a mechanism to comment on existing and proposed legislation and regulations that have government-wide impact.

During this reporting period, we reviewed more than 100 legislative and regulatory proposals, draft DHS policy directives, and other items. Three of these items are summarized below.

DHS Proposed Categories of Controlled Unclassified Information
In November 2010, Executive Order 13556, "Controlled Unclassified Information," (CUI) was issued to establish a uniform program for consistently categorizing, marking, and safeguarding "Sensitive But Unclassified" (SBU) information within the executive branch. The Executive Order requires agencies to provide the National Archives and Records Administration (NARA) with a list of proposed categories of SBU information meriting "CUI" designation. NARA is required to review each agency's proposal, and establish and maintain a government-wide registry of "authorized" CUI categories, associated markings, and applicable safeguarding procedures.

In April 2011, to comply with the Executive Order, DHS asked each component to propose categories of information that merit safeguarding as CUI. The OIG proposed several categories for the Department's consideration. Later that month, the OIG reviewed and commented on the Department's consolidated list of proposed CUI categories drafted for NARA's review.

Faster FOIA Act of 2011
Our office reviewed this proposed legislation and made specific recommendations premised on OIG's experience in processing complex FOIA requests.

Digital Accountability and Transparency Act of 2011
Our office reviewed and commented on this draft CIGIE legislation, ultimately making recommendations based on OIG authorities.

CONGRESSIONAL TESTIMONY AND BRIEFINGS

The Inspector General testified before congressional committees twice during this time period. Testimony prepared for this hearing may be accessed on our website at **www.oig.dhs.gov/**.

We testified on the following issues:

- June 9, 2011—Senate Homeland Security and Governmental Affairs Committee, Subcommittee on Disaster Recovery and Intergovernmental Affairs on the corruption of DHS employees working along the southwest border.

- July 15, 2011—House Committee on Homeland Security, Subcommittee on Oversight, Investigations and Management on whether the Department effectively leveraged emerging technologies.

We briefed congressional members and their staffs at a steady pace throughout the reporting period. Our office conducted more than 25 briefings for congressional staff on the results of our work, including: (1) Customs and Border Protection's Ground Transportation of Detainees (OIG-11-27); (2) Transportation Security Administration (TSA) Vetting of Airmen Certificates and General Aviation Airport Access and Security Procedures (OIG-11-96); (3) TSA's Oversight of the Airport Badging Process Needs Improvement (OIG-11-95); and (4) Planning, Management, and Systems Issues Hinder DHS' Efforts To Protect Cyberspace and the Nation's Cyber Infrastructure (OIG-11-89). We attended meetings to discuss other congressional concerns, including a request to review TSA's Screening Partnership Program, a briefing regarding the Secure Communities Program, and a briefing to discuss OIG's role in disaster work.

We will continue to meet with congressional members and staff to discuss our evaluations of the Department's programs and operations and to brief them on completed and planned work.

APPENDIXES

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	162	$353,980,852	$73,099,003
Plus prior period adjustments (a)	0	$633,285	$0
B. Reports issued/processed during the reporting period with questioned costs	26	$855,383,832	$62,263,057
Total Reports (A+B)	**188**	**$1,209,997,969**	**$135,362,060**
C. Reports for which a management decision was made during the reporting period (b)	35	$91,405,052	$19,095,361
(1) Disallowed costs	34	$27,821,809	$541,435
(2) Accepted costs	20	$63,583,243	$18,553,926
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	$1,118,592,917	$116,266,699
F. Reports for which no management decision was made within 6 months of issuance	127	$263,209,085	$54,003,642

Notes and Explanations:

(a) Adjustments were made to account for disaster assistance audit reports not previously accounted.

(b) Report totals in Section C may not always equal the total in lines C (1) and C (2) because some reports contain both allowed and disallowed costs. In addition, resolution may result in values different from the original recommendations.

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 – Previously questioned costs accepted in a management decision as allowable costs to a government program. Before acceptance, we must agree with the basis for the management decision.

Questioned Costs – Auditors questioning costs resulting from alleged violations of provisions of laws, regulations, grants, cooperative agreements, or contracts. A "questioned" cost is a finding 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 – Costs 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	38	$71,176,821
B. Reports issued during the reporting period	12	$10,302,337
Total Reports (A+B)	**50**	**$81,479,158**
C. Reports for which a management decision was made during the reporting period (a)	10	$4,662,522
(1) Value of recommendations agreed to by management for deobligation	10	$4,314,622
(2) Value of recommendations not agreed to by management	1	$347,900
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	40	$76,816,636
F. Reports for which no management decision was made within 6 months of issuance	28	$66,514,299

Notes and Explanations:

(a) Report totals in Section C may not always equal the total in lines C (1) and C (2) because some reports contain both allowed and disallowed costs. In addition, resolution may result in values different from the original recommendations.

Funds Put to Better Use – Auditors can identify ways to improve the efficiency, effectiveness, and economy of programs, resulting in cost 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 [a]

MANAGEMENT DECISION IS PENDING	
3/31/11	
Reports open and unresolved more than 6 months	164
Recommendations open and unresolved more than 6 months	534
9/30/11	
Reports open and unresolved more than 6 months	173
Recommendations open and unresolved more than 6 months	691
CURRENT INVENTORY	
Open reports at the beginning of the period	363
Reports issued this period	82
Reports closed this period	81
Open reports at the end of the period	364
ACTIVE RECOMMENDATIONS	
Open recommendations at the beginning of the period	1,691
Recommendations issued this period	301
Recommendations closed this period	329
Open recommendations at the end of the period	1,663

[a] Includes management & financial assistance grants issued.

Appendix 3
Management Reports Issued

Report Number	Date Issued	Report Title	Questioned Costs	Unsupported Costs	Funds Put to Better Use
1. OIG-11-68	4/11	Information Sharing on Foreign Nationals: Overseas Screening (Redacted)	$0	$0	$0
2. OIG-11-69	4/11	Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology	$0	$0	$0
3. OIG-11-70	4/11	Information Technology Management Letter for the Immigration and Customs Enforcement Component of the FY 2010 DHS Financial Statement Audit	$0	$0	$0
4. OIG-11-71	4/11	DHS Oversight of Component Acquisition Programs	$0	$0	$0
5. OIG-11-72	4/11	Special Report: Summary of Significant Investigations October 1, 2009 to December 31, 2010	$0	$0	$0
6. OIG-11-73	4/11	Information Technology Management Letter for the Transportation Security Administration Component of the FY 2010 DHS Financial Statement Audit	$0	$0	$0
7. OIG-11-74	4/11	Information Technology Management Letter for the U.S. Citizenship and Immigration Services Component of the FY 2010 DHS Financial Statement Audit	$0	$0	$0
8. OIG-11-75	4/11	Federal Emergency Management Agency's Management Letter for FY 2010 DHS Consolidated Financial Statements Audit	$0	$0	$0
9. OIG-11-76	4/11	Information Technology Management Letter for the Federal Law Enforcement Training Center Component of the FY 2010 DHS Financial Statement Audit	$0	$0	$0
10. OIG-11-77	4/11	Opportunities to Improve FEMA's Mass Care and Emergency Assistance Activities	$0	$0	$0

Appendix 3
Management Reports Issued (continued)

Report Number	Date Issued	Report Title	Questioned Costs	Unsupported Costs	Funds Put to Better Use
11. OIG-11-78	4/11	Design and Implementation of the Federal Emergency Management Agency's Emergency Management Performance Grant	$0	$0	$0
12. OIG-11-79	5/11	Information Technology Management Letter for the Federal Emergency Management Agency Component of the FY 2010 DHS Financial Statement Audit	$0	$0	$0
13. OIG-11-80	5/11	Information Technology Management Letter for the United States Coast Guard Component of the FY 2010 DHS Financial Statement Audit	$0	$0	$0
14. OIG-11-81	5/11	Supervision of Aliens Commensurate with Risk	$0	$0	$0
15. OIG-11-82	5/11	U.S. Coast Guard's Anti-Deficiency Act Violations for the Response Boat-Medium Major Acquisition Project for Fiscal Years 2004 Through 2009	$0	$0	$0
16. OIG-11-83	5/11	The State of Nevada's Management of State Homeland Security Program and Urban Areas Security Initiative Grants Awarded During Fiscal Years 2006 through 2008	$0	$0	$0
17. OIG-11-84	5/11	Assessment of FEMA's Fraud Prevention Efforts	$643,000,000	$0	$0
18. OIG-11-85	5/11	U.S. Citizenship and Immigrations Services Privacy Stewardship	$0	$0	$0
19. OIG-11-86	6/11	U.S. Coast Guard's Marine Safety Program – Offshore Vessel Inspections	$0	$0	$0
20. OIG-11-87	6/11	Management Oversight and Additional Automated Capabilities Needed to Improve Intelligence Information Sharing (Redacted)	$0	$0	$0

Appendix 3
Management Reports Issued (continued)

Report Number	Date Issued	Report Title	Questioned Costs	Unsupported Costs	Funds Put to Better Use
21. OIG-11-89[1]	6/11	Planning, Management, and Systems Issues Hinder DHS' Efforts To Protect Cyberspace and the Nation's Cyber Infrastructure (Redacted)	$0	$0	$0
22. OIG-11-90	6/11	Information Technology Management Letter for the FY 2010 U.S. Customs and Border protection Financial Statement Audit (Redacted)	$0	$0	$0
23. OIG-11-91	6/11	Update on DHS' Procurement and Program Management Operations	$0	$0	$0
24. OIG-11-92	6/11	Efficacy of Customs and Border Protection's Bonding Process	$0	$0	$0
25. OIG-11-93	6/11	DHS Grants Used for Mitigating Risks to Amtrak Rail Stations	$0	$0	$0
26. OIG-11-94	7/11	DHS/U.S. Secret Service FY 2009 Antideficiency Act Violation	$0	$0	$0
27. OIG-11-95	7/11	TSA's Oversight of the Airport Badging Process Needs Improvement (Redacted)	$0	$0	$0
28. OIG-11-96	7/11	Transportation Security Administration (TSA) Vetting of Airmen Certificates and General Aviation Airport Access and Security Procedures	$0	$0	$0
29. OIG-11-97	7/11	Use of American Recovery and Reinvestment Act Funds by U.S. Customs and Border Protection for Construction of Land Ports of Entry	$0	$0	$0

[1] OIG-11-88 "Compendium of Disaster Preparedness Programs" was issued on behalf of CIGIE and was not a management report issued to the Department.

Appendix 3
Management Reports Issued (continued)

Report Number	Date Issued	Report Title	Questioned Costs	Unsupported Costs	Funds Put to Better Use
30. OIG-11-98	7/11	Evaluation of DHS' Security Program and Practices for Intelligence Systems for Fiscal Year 2011	$0	$0	$0
31. OIG-11-99	7/11	Improvements in Patch and Configuration Management Controls Can Better Protect TSA's Wireless Network and Devices (Redacted)	$0	$0	$0
32. OIG-11-100	7/11	DHS Detainee Removals and Reliance on Assurances	$0	$0	$0
33. OIG-11-101	8/11	Use of DHS Purchase Cards	$0	$0	$0
34. OIG-11-102	8/11	Effectiveness and Costs of FEMA's Disaster Housing Assistance Program	$0	$0	$0
35. OIG-11-103	8/11	Information Technology Management Letter for the FY 2010 DHS Financial Statement Audit (Redacted)	$0	$0	$0
36. OIG-11-104	8/11	Review of Costs Invoiced by the City of San Francisco Relating to the Terminal 2 Checked Baggage Screening Project at San Francisco International Airport Under Other Transaction Agreement Number HSTS04-09-H-REC123	$303,474	$303,474	$0
37. OIG-11-105	8/11	The U.S. Citizenship and Immigration Services' Adjudication of Petitions for Nonimmigrant Workers (I-129 Petitions for H-1B and H-2B visas)	$0	$0	$0
38. OIG-11-106	8/11	FEMA's Contracting Officer's Technical Representative Program	$0	$0	$0

Appendix 3
Management Reports Issued (continued)

Report Number	Date Issued	Report Title	Questioned Costs	Unsupported Costs	Funds Put to Better Use
39. OIG-11-107	9/11	DHS' Role in Nominating Individuals for Inclusion on the Government Watchlist and Its Efforts to Support Watchlist Maintenance	$0	$0	$0
40. OIG-11-108	9/11	Coast Guard Has Taken Steps to Strengthen Information Technology Management, but Challenges Remain	$0	$0	$0
41. OIG-11-109	9/11	The Commonwealth of Pennsylvania's Management of State Homeland Security Program and Urban Areas Security Initiative Grants Awarded During Fiscal Years 2007 through 2009	$0	$0	$0
42. OIG-11-110	9/11	DHS Risk Assessment Efforts in the Dams Sector	$0	$0	$0
43. OIG-11-111	9/11	Annual Review of the United States Coast Guard's Mission Performance (FY 2010)	$0	$0	$0
44. OIG-11-112	9/11	The State of New Jersey's Management of State Homeland Security Program and Urban Areas Security Initiative Grants Awarded During Fiscal Years 2007 through 2009	$2,657,212	$861,044	$585,519
45. OIG-11-113	9/11	Evaluation of DHS' Information Security Program for Fiscal Year 2011	$0	$0	$0
46. OIG 11-114	9/11	Improving FEMA's Individual Assistance, Technical Assistance Contracts	$0	$0	$0
47. OIG-11-115	9/11	United States Coast Guard's Internal Controls and Cost Capturing for the Deepwater Horizon Oil Spill	$0	$0	$0

Appendix 3
Management Reports Issued (continued)

Report Number	Date Issued	Report Title	Questioned Costs	Unsupported Costs	Funds Put to Better Use
48. OIG-11-116	9/11	DHS Continues to Face Challenges in the Implementation of Its OneNet Project	$0	$0	$0
49. OIG-11-117	9/11	Review of the Department of Homeland Security's Capability to Share Cyber Threat Information	$0	$0	$0
50. OIG-11-118	9/11	Security Issues with U.S. Customs and Border Protection's Enterprise Wireless Infrastructure	$0	$0	$0
51. OIG-11-119[a]	9/11	The Performance of 287(g) Agreements FY 2011 Update	$0	$0	$0
		Total, Appendix 3	**$645,960,686**	**$1,164,518**	**$585,519**

[a] OIG-11-120 "Recommended Practices for Office of Inspectors General Use of New Media" and OIG-11-121 "Management Advisory Report on Cybersecurity" were issued on behalf of CIGIE and was not a management report issued to the Department.

Appendix 4

Financial Assistance Audit Reports Issued

Report Number	Date Issued	Report Title	Questioned Costs	Unsupported Costs	Funds Put to Better Use
1. DA-11-12	4/11	Mississippi State Port Authority	$3,215,475	$2,786,000	$1,335,495
2. DA-11-13	4/11	City of Deerfield Beach, Florida	$3,928,753	$0	$0
3. DA-11-14	4/11	North Carolina Department of Transportation – Disaster Activities Related to Tropical Storm Frances	$47,321	$0	$0
4. DA-11-15	4/11	North Carolina Department of Transportation-Disaster Activities Related to Hurricane Ivan	$682,325	$0	$0
5. DA-11-16	5/11	Coast Transit Authority	$0	$0	$223,744
6. DA-11-17	5/11	Florida International University	$927,446	$0	$0
7. DA-11-18	5/11	City of Vero Beach, Florida – Disaster Activities Related to Hurricane Jeanne	$1,266,084	$441,125	$0
8. DA-11-19	5/11	City of Vero Beach, Florida – Disaster Activities Related to Hurricane Frances	$2,333,541	$316,755	$0
9. DA-11-20	8/11	FEMA Public Assistance Grant Funds Awarded to Gulf Shores Utilities, Gulf Shores, Alabama	$0	$0	$0
10. DA-11-21	8/11	FEMA Public Assistance Grant Funds Awarded to Memorial Hospital at Gulfport, Mississippi	$0	$0	$0
11. DA-11-22	8/11	FEMA Public Assistance Grant Funds Awarded to City of Mobile, Alabama	$0	$0	$0
12. DA-11-23	8/11	FEMA Public Assistance Grant Funds Awarded to Gulf Coast Community Action Agency, Gulfport, Mississippi	$2,724,633	$0	$2,293,832

Appendix 4
Financial Assistance Audit Reports Issued (continued)

Report Number	Date Issued	Report Title	Questioned Costs	Unsupported Costs	Funds Put to Better Use
13. DA-11-24	9/11	FEMA Public Assistance Grant Funds Awarded to Wayne County, Mississippi, Board of Supervisors	$7,327,370	$0	$0
14. DD-11-12	4/11	Xavier University of Louisiana	$75,352,011	$25,648,720	$0
15. DD-11-13	4/11	City of Austin, Texas	$623,722	$0	$0
16. DD-11-14	4/11	South Central Power Company, Ohio	$0	$0	$0
17. DD-11-15	8/11	FEMA Public Assistance Grant Funds Awarded to Saint Mary's Academy, New Orleans, Louisiana	$51,138,010	$0	$0
18. DD-11-16	8/11	Interim Report on FEMA Public Assistance Grant Funds Awarded to Regional Transit Authority, New Orleans, Louisiana	$31,740,000	$31,740,000	$0
19. DD-11-17	8/11	Capping Report: FY 2010 FEMA Public Assistance Grant and Subgrant Audits	$0	$0	$0
20. DD-11-18	8/11	FEMA Public Assistance Grant Funds Awarded to Iowa Department of Transportation	$36,330	$0	$0
21. DD-11-19	8/11	FEMA Public Assistance Grant Funds Awarded to Port of New Orleans, Louisiana	$2,600,000	$0	$670,974
22. DD-11-20	9/11	FEMA Public Assistance Grant Funds Awarded to Calcasieu Parish School Board, Lake Charles, Louisiana	$3,668,790	$22,610	$747,016
23. DD-11-21	9/11	FEMA Public Assistance Grant Funds Awarded to Jesuit High School, New Orleans, Louisiana	$11,585,610	$4,293	$27,518

Appendix 4
Financial Assistance Audit Reports Issued (continued)

Report Number	Date Issued	Report Title	Questioned Costs	Unsupported Costs	Funds Put to Better Use
24. DD-11-22	9/11	FEMA Public Assistance Grant Funds Awarded to Henderson County, Illinois	$3,230,378	$0	$0
25. DD-11-23	9/11	FEMA Region VI Audit Follow-up and Resolution Activities	$0	$0	$0
26. DD-11-24	9/11	FEMA Public Assistance Grant Funds Awarded to Orleans Parish Criminal Sheriff's Office, Louisiana	$3,532,607	$99,242	$285,771
27. DS-11-09	7/11	Reclamation District 768, Arcata, California	$1,565,975	$0	$1,420,757
28. DS-11-10	8/11	FEMA Public Assistance Funds Awarded to County of Humboldt, California	$671,652	$0	$175,510
29. DS-11-11	9/11	FEMA Public Assistance Grant Funds Awarded to City of Petaluma, California	$0	$0	$1,629,386
30. DS-11-12	9/11	FEMA Public Assistance Grant Funds Awarded to City of Paso Robles, California	$833,215	$38,912	$0
31. DS-11-13	9/11	FEMA Public Assistance Grant Funds Awarded to County of Sonoma, California	$391,898	$882	$906,815
		Total, Appendix 4	**$209,423,146**	**$61,098,539**	**$9,716,818**

Report Number Acronyms:

DA Financial Assistance Disaster Audit, Atlanta Office
DD Financial Assistance Disaster Audit, Dallas Office
DS Financial Assistance Disaster Audit, Oakland Office

Appendix 5
Schedule of Amounts Due and Recovered

Report Number	Date Issued	Auditee	Amount Due	Recovered Costs
1. DS-08-08	9/08	State of California Administration of the Fire Management Assistance Grant Program for the Canyon Fire	$386,573	$330,033
2. DA-09-19	7/09	Hurricane Katrina Activities for Pass Christian Public School District	$333,432	$134,486
3. DA-09-21	8/09	Hurricane Georges Activities for Puerto Rico Electric and Power Authority	$15,120,502	$14,006,987
4. DA-10-03	12/09	City of Biloxi, Mississippi	$224,466	$22,750
5. DS-10-01	1/10	County of Santa Cruz, California	$55,888	$55,888
6. DA-10-04	1/10	City of Moss Point, Mississippi	$133,016	$133,016
7. DD-10-06	3/10	Town of Vinton, Louisiana	$188,329	$223,637
8. DD-10-09	4/10	City of Bucyrus, Ohio	$27,041	$3,276
9. DD-10-10	6/10	Nebraska Public Power District, Columbus, Nebraska	$1,662,599	$1,646,779
10. DA-10-14	7/10	Hancock County School District	$59,312	$59,312
11. DD-11-01	10/10	University of Texas, MD Anderson Cancer Center	$447,502	$313,857
12. DD-11-10	3/11	City of Port Arthur, Texas	$262,967	$262,967
13. INV	4/11 through 9/11	Recoveries as a result of investigations	$2,664,516	$2,664,516
		Total, Appendix 5	**$21,566,143**	**$ 19,857,504**

Report Number Acronyms:

DA Financial Assistance Disaster Audit, Atlanta Office
DD Financial Assistance Disaster Audit, Dallas Office
DS Financial Assistance Disaster Audit, Oakland Office
INV Recoveries, other than administrative cost savings, which resulted from investigative efforts

Appendix 6[2]

Contract Audit Reports

Report Category	Questioned Costs	Unsupported Costs	Disallowed Costs
We processed no contract audit reports meeting the criteria of the *National Defense Authorization Act for FY 2008* during the reporting period April 1, 2011 - September 30, 2011	N/A	N/A	N/A

[2] The *National Defense Authorization Act for FY 2008* requires that we list all contract audit reports issued during the reporting period containing significant audit findings; briefly describe the significant audit findings in the report; and specify the amounts of costs identified in the report as unsupported, questioned, or disallowed. This act defines significant audit findings as unsupported, questioned, or disallowed costs in excess of $10,000,000, or other findings that the Inspector General determines to be significant. It defines contracts as a contract, an order placed under a task or delivery order contract, or a subcontract.

Appendix 7
Peer Review Results

Section 989C of the *Dodd-Frank Wall Street Reform and Consumer Protection Act*, P.L. 111-203 (2010), contains additional semiannual reporting requirements pertaining to peer review reports of OIG operations. Federal Inspectors General are required to engage in peer review processes related to both their audit and investigative operations. In keeping with section 989C, our office is reporting the following information related to peer reviews of our operations conducted by other Inspectors General. We are also including information about peer reviews we conducted of the activities of other OIGs.

For audits, peer reviews of audit organization's system of quality controls are conducted on a 3-year cycle. These reviews are conducted according to the CIGIE *Guide for Conducting External Peer Reviews of the Audit Organization of Federal Offices of Inspector General*, and are based on requirements established by the GAO in its Government Auditing Standards (Yellow Book). Federal audit organizations can receive a rating of pass, pass with deficiencies, or fail.

For investigations, quality assessment peer reviews of investigative operations are conducted on a 3-year cycle. Such reviews result in a determination that an organization is "in compliance" or "not in compliance" with relevant standards. These standards are based on Quality Standards for Investigations and applicable Attorney General guidelines. The Attorney General guidelines include the *Attorney General Guidelines for Offices of Inspectors General with Statutory Law Enforcement Authority* (2003), *Attorney General Guidelines for Domestic Federal Bureau of Investigation Operations* (2008), and *Attorney General Guidelines Regarding the Use of Confidential Informants* (2002).

Audits

Peer Review Conducted on DHS OIG Audit Operations
DHS OIG audit offices received a peer review rating of "pass" resulting from a peer review conducted by the Department of Labor OIG for fiscal year ending September 2008. Two recommendations from that review remain open:

1. DHS OIG revise its Audit Manual to include the requirements of Generally Accepted Government Auditing Standards (GAGAS) paragraphs 7.57 and 7.59.

Overall Status: Resolved. DHS OIG's 2008 Audit Manual Addendum includes implementing policy and guidance related to GAGAS 7.57 and 7.59. We agreed to enhance our guidance in our next audit manual. Our new manual was to be issued in the fourth quarter of FY 2011. We did not issue our new manual as planned because GAO announced plans to issue a revised Yellow Book by December 15, 2011. We postponed the issuance of our new audit manual to allow ourselves time to incorporate additional guidance needed to comply with GAO's revised guidance. We anticipate issuing a new audit manual by the second quarter of FY 2012.

2. DHS OIG emphasize to audit staff the requirement to document the consideration for fraud, starting in the audit planning phase. As an additional control, the Supervisory Review Checklist should be expanded to include that requirement.

Overall Status: Resolved. Shortly after receiving the recommendation, all DHS OIG auditors were notified to better document fraud consideration through training classes and daily supervisory guidance. Again this Semiannual Report period, DHS OIG auditors were reminded to follow these requirements during audit office staff meetings. As an additional control, the Supervisory Review Checklist will be expanded and a new checklist will be issued in the first quarter of FY 2012.

Peer Review Conducted by DHS OIG on other OIG Audit Operations
DHS OIG conducted a peer review on the Environmental Protection Agency (EPA) OIG Office of Audits for fiscal year ending September 2008. EPA OIG Office of Audits received a peer review rating of "pass." No recommendations were issued.

Investigations

Peer Review Conducted on DHS OIG Investigative Operations
DHS OIG Office of Investigations received a peer review conducted by the Social Security Administration OIG for fiscal year ending September 2009. We received a peer review rating of "in compliance." No recommendations were issued.

Peer Review Conducted by DHS OIG on other OIG Investigative Operations
DHS OIG Office of Investigations conducted a peer review on the U.S. Department of Agriculture (USDA) OIG for fiscal year ending 2010. The USDA OIG received a peer review rating of "in compliance." No recommendations were issued.

Appendix 8
Acronyms

A&E	architectural and engineering
ADA	*Anti-Deficiency Act*
AEMA	Alabama Emergency Management Agency
AICPA	American Institute of Certified Public Accountants
AO	Adjudication Officer
BPA	Border Patrol Agent
Cal EMA	California Emergency Management Agency
CAT	Convention Against Torture and other Cruel, Inhuman, or Degrading Treatment or Punishment
CBP	United States Customs and Border Protection
CFO	Chief Financial Officer
CPSB	Calcasieu Parish School Board
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CLAIMS	Computer Linked Application Information Management System
CO	Correctional Officer
COTR	contracting officer's technical representatives
CTA	Coast Transit Authority
CUI	Controlled Unclassified Information
DHAP	Disaster Housing Assistance Program
DHS	Department of Homeland Security
DoD	Department of Defense
DOT	Department of Transportation
DRA	Detention and Removal Assistant
DRO	Detention and Removal Officer
EMA	Emergency Management Agency
EMO	Office of Emergency Management Oversight
EMPG	Emergency Management Performance Grant
EPA	Environmental Protection Agency
EWI	Enterprise Wireless Infrastructure
FAA	Federal Aviation Administration
FAMS	Federal Air Marshal Service
FDEM	Florida Division of Emergency Management
FEMA	Federal Emergency Management Agency
FLETC	Federal Law Enforcement Training Center
FOIA	*Freedom of Information Act*
FPIB	Fraud Prevention and Investigative Branch
FPS	Federal Protective Service
FY	fiscal year
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office

Appendix 8
Acronyms (continued)

GOHSEP	Governor's Office of Homeland Security and Emergency Preparedness
HMGP	Hazard Mitigation Grant Program
HUD	Department of Housing and Urban Development
I&A	Office of Intelligence and Analysis
IA-TACS	Individual Assistance, Technical Assistance Contracts
ICE	United States Immigration and Customs Enforcement
INV	Office of Investigations
ISO	Immigration Services Officer
ISP	Office of Inspections
IT	information technology
ITA	Office of Information Technology Audits
ITGC	information technology general control
MEMA	Mississippi Emergency Management Agency
MSPA	Mississippi State Port Authority
NARA	National Archives and Records Administration
NCDEM	North Carolina Division of Emergency Management
NPPD	National Protection and Program Directorate
OA	Office of Audits
OC	Office of Counsel to the Inspector General
OIG	Office of Inspector General
OLA	Office of Legislative Affairs
OM	Office of Management
OMB	Office of Management and Budget
OPA	Office of Public Affairs
PA	Public Assistance
PII	personally identifiable information
POA&M	plans of action and milestones
PONO	Port of New Orleans
POE	port of entry
RTA	Regional Transit Authority (New Orleans)
SBA	Small Business Administration
SBU	sensitive but unclassified
SCP	South Central Power Company, Ohio
SMA	St. Mary's Academy
TSA	Transportation Security Administration
TSDB	Terrorist Screening Database
TSO	Transportation Security Officer
TSDB	Terrorist Screening Database
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Services
USDA	United States Department of Agriculture
USSS	United States Secret Service

Appendix 9
OIG Headquarters/Field Office Contacts and Locations

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

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

OIG Headquarters Senior Management Team	
Charles K. Edwards	Acting Inspector General
Yvonne Manino	Acting Chief of Staff
Dorothy Balaban	Special Assistant
Richard N. Reback	Counsel to the Inspector General
Matthew Jadacki	Assistant Inspector General/Emergency Management Oversight
Anne L. Richards	Assistant Inspector General/Audits
Thomas M. Frost	Assistant Inspector General/Investigations
Carlton I. Mann	Assistant Inspector General/Inspections
Frank Deffer	Assistant Inspector General/Information Technology Audits
Louise McGlathery	Acting Assistant Inspector General/Management
Philip D. McDonald	Acting Director, Office of Legislative Affairs
Marta R. Metelko	Director, Office of Public Affairs

Appendix 9

OIG Headquarters/Field Office Contacts and Locations (continued)

Locations of OA Field Offices

Boston, MA
Boston, MA 02222
(617) 565-8700 / Fax (617) 565-8996

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

Denver, CO
Denver, CO 80225
(303) 236-2878/ Fax (303) 236-2880

Houston, TX
Houston, TX 77057
(713) 212-4350 / Fax (713) 212-4361

Miami, FL
Miramar, FL 33027
(954) 538-7840 / Fax (954) 602-1034

Philadelphia, PA
Marlton, NJ 08053
(856) 596-3810 / Fax (856) 810-3412

Location of ITA Field Office

Seattle, WA
Kirkland, WA 98033
(425) 250-1363

Locations of EMO Field Offices

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

Biloxi, MS
Biloxi, MS 39531
(228) 822-0563 / Fax (228) 822-0296

Dallas, TX
Frisco, TX 75034
(214) 436-5200 / Fax (214) 436-5201

New Orleans, LA
New Orleans, LA 70114
(504) 762-2050 / Fax (504) 762-2388

Oakland, CA
Oakland, CA 94612
(510) 637-4311 / Fax (510) 637-1487

San Juan, PR
San Juan, PR 00918
(787) 294-2532 / Fax (787) 771-3617

Appendix 9

OIG Headquarters/Field Office Contacts and Locations (continued)

Alpine, TX
Alpine, TX 79830
(432) 837-7332 / Fax: (432) 837-7449

Atlanta, GA
Atlanta, GA 30341
(404) 832-6730 / Fax: (404) 832-6646

Baton Rouge, LA
Baton Rouge, LA 70803
(225) 334-4900 / Fax: (225) 578-4982

Bellingham, WA
Bellingham, WA 98226
(360) 527-4400 Fax: (360) 671-0576

Biloxi, MS
Biloxi, MS 39531
(228) 385-9215 / Fax: (228) 385-9220

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

Buffalo, NY
Buffalo, NY 14202
(716) 551-4231 / Fax: (716) 551-4238

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

Dallas, TX
Frisco, TX 75034
(214) 436-5250 / Fax: (214) 436-5276

Del Rio, TX
Del Rio, TX 78840
(830) 298-2629 x239 / Fax: (830) 298-3282

Denver, CO
Castle Rock, CO 80104
(303) 653-1627 / Fax (not available)

Detroit, MI
Detroit, MI 48126
(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

Hattiesburg, MS
Hattiesburg, MS 39402-8881
(601) 264-8220 / Fax: (601) 264-9088

Houston, TX
Houston, TX 77027
(713) 212-4300 / Fax: (713) 212-4363

Laredo, TX
Laredo, TX 78045
(956) 794-2917 / Fax: (956) 717-0395

Los Angeles, CA
El Segundo, CA 90245
(310) 665-7320 / Fax: (310) 665-7309

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

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

Mobile, AL
Mobile, AL 36609
(251) 415-3278 / Fax: (251) 219-3517

New Orleans, LA
New Orleans, LA 70114
(504) 762-2202 / Fax: (504) 762-2376

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

Orlando, FL
Orlando, Fl 32809-7892
(407) 506-1950 / Fax (407) 240-8104

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

San Diego, CA
San Diego, CA 92101
(619) 235-2501 / Fax: (619) 687-3144

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) 250-1360 / Fax: (425) 576-0898

Sierra Vista, AZ
Sierra Vista, AZ 85635
(520) 229-6420 / Fax: (520) 742-7192

Tucson, AZ
Tucson, AZ 85741
(520) 229-6420 / Fax: (520) 742-7192

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

Yuma, AZ
Yuma, AZ 85364
(928) 373-1620 / Fax: (928) 783-0477

Appendix 10

Index to Reporting Requirements

The specific reporting requirements described in the *Inspector General Act of 1978*, as amended, including Section 989C of the *Dodd-Frank Wall Street and Consumer Protection Act*, are listed below with a reference to the Semiannual Report to Congress pages on which they are addressed.

Requirements:	Pages
Review of Legislation and Regulations	54-55
Significant Problems, Abuses, and Deficiencies	10-48
Recommendations With Significant Problems	10-48
Prior Recommendations Not Yet Implemented	52
Matters Referred to Prosecutive Authorities	Statistical Highlights
Summary of Instances Where Information Was Refused	N/A
List of Audit Reports	62-70
Summary of Significant Audits	10-48
Reports With Questioned Costs	59
Reports Recommending That Funds Be Put to Better Use	60
Summary of Reports in Which No Management Decision Was Made	59-60
Revised Management Decisions	N/A
Management Decision Disagreements	N/A
Peer Review Results	73

U.S. DEPARTMENT OF HOMELAND SECURITY

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) 254-4305, or visit the OIG website at www.oig.dhs.gov/

OIG Hotline

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

CALL our Hotline at 1-800-323-8603;

FAX the complaint directly to us at (202) 254-4292;

EMAIL us at DHSOIGHOTLINE@dhs.gov; or

WRITE to us at:
DHS Office of Inspector General/MAIL STOP 2600
Attention: Office of Investigations – Hotline
245 Murray Drive SW, Building 410
Washington, DC 20528

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