



Department of Homeland Security  
**OFFICE OF INSPECTOR GENERAL**

*Safeguarding and Securing Cyberspace*

**SEMIANNUAL  
REPORT TO  
THE CONGRESS**

**April 1, 2010 through September 30, 2010**

# Statistical Highlights of OIG Activities

## April 1, 2010 through September 30, 2010

### Dollar Impact

Questioned Costs	\$77,597,951
Funds Put to Better Use	\$53,241,230
Management Agreement That Funds Be:	
Recovered	\$4,438,714
Deobligated	\$25,613,545
Funds Recovered (from audits and investigations)	\$3,687,304
Fines, Restitutions, and Administrative Cost Savings	\$6,508,342

### Activities

Management Reports Issued	48
Financial Assistance Grant Audit Reports	29
Investigative Reports Issued	546
Investigations Initiated	694
Investigations Closed	600
Open Investigations	2,086
Investigations Referred for Prosecution	223
Investigations Accepted for Prosecution	143
Investigations Declined for Prosecution	57
Arrests	198
Indictments	154
Convictions	115
Personnel Actions	89
Complaints Received (other than Hotline)	6,312
Hotline Complaints Received	5,037
Complaints Referred (to programs or other agencies)	6,631
Complaints Closed	8,376

Office of Inspector General

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



**Homeland  
Security**

October 29, 2010

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 for the 6-month period ended September 30, 2010.

During this reporting period, our office published 48 management reports and 29 financial assistance grant reports. DHS management concurred with 95% of recommendations contained in our management reports. As a result of these efforts, \$77.6 million of questioned costs were identified, of which \$25 million were determined to be unsupported. We recovered \$3.7 million as a result of disallowed costs identified from previous audit reports and from investigative efforts. We issued 10 reports identifying \$53.2 million in funds put to better use. In addition, management agreed to deobligate \$25.6 million in disaster grant assistance, which will result in funds put to better use.

In the investigative area, we issued 546 investigative reports, initiated 694 investigations, and closed 600 investigations. Our investigations resulted in 198 arrests, 154 indictments, 115 convictions, and 89 personnel actions. Additionally, we reported \$6.5 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,

A handwritten signature in black ink that reads "Richard L. Skinner".

Richard L. Skinner  
Inspector General



# Table of Contents

<b>STATISTICAL HIGHLIGHTS OF OFFICE OF INSPECTOR GENERAL ACTIVITIES .....</b>	<b>INSIDE COVER</b>
<b>INSPECTOR GENERAL’S MESSAGE .....</b>	<b>1</b>
<b>WORKING RELATIONSHIP PRINCIPLES FOR AGENCIES AND OFFICES OF INSPECTOR GENERAL .....</b>	<b>4</b>
<b>EXECUTIVE SUMMARY .....</b>	<b>5</b>
<b>DEPARTMENT OF HOMELAND SECURITY PROFILE .....</b>	<b>6</b>
<b>OFFICE OF INSPECTOR GENERAL PROFILE .....</b>	<b>7</b>
<b>SUMMARY OF SIGNIFICANT OFFICE OF INSPECTOR GENERAL ACTIVITY .....</b>	<b>10</b>
<b>DIRECTORATE FOR MANAGEMENT .....</b>	<b>11</b>
<b>DIRECTORATE FOR NATIONAL PROTECTION AND PROGRAMS .....</b>	<b>13</b>
<b>DIRECTORATE FOR SCIENCE AND TECHNOLOGY .....</b>	<b>14</b>
<b>FEDERAL EMERGENCY MANAGEMENT AGENCY .....</b>	<b>14</b>
<b>FEDERAL LAW ENFORCEMENT TRAINING CENTER .....</b>	<b>25</b>
<b>OFFICE FOR CIVIL RIGHTS AND CIVIL LIBERTIES .....</b>	<b>26</b>
<b>OFFICE OF COUNTERNARCOTICS ENFORCEMENT .....</b>	<b>26</b>
<b>TRANSPORTATION SECURITY ADMINISTRATION .....</b>	<b>26</b>
<b>UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES .....</b>	<b>27</b>
<b>UNITED STATES COAST GUARD .....</b>	<b>29</b>
<b>UNITED STATES CUSTOMS AND BORDER PROTECTION .....</b>	<b>32</b>
<b>UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT .....</b>	<b>36</b>
<b>MULTIPLE COMPONENTS .....</b>	<b>39</b>
<b>OTHER OFFICE OF INSPECTOR GENERAL ACTIVITIES .....</b>	<b>42</b>
<b>LEGISLATIVE AND REGULATORY REVIEWS .....</b>	<b>44</b>
<b>CONGRESSIONAL TESTIMONY AND BRIEFINGS .....</b>	<b>46</b>
<b>APPENDICES .....</b>	<b>48</b>
<b>APPENDIX 1      AUDIT REPORTS WITH QUESTIONED COSTS .....</b>	<b>49</b>
<b>APPENDIX 1B     AUDIT REPORTS WITH FUNDS PUT TO BETTER USE .....</b>	<b>50</b>
<b>APPENDIX 2      COMPLIANCE—RESOLUTION OF REPORTS AND RECOMMENDATIONS .....</b>	<b>51</b>
<b>APPENDIX 3      MANAGEMENT REPORTS ISSUED .....</b>	<b>52</b>
<b>APPENDIX 4      FINANCIAL ASSISTANCE AUDIT REPORTS ISSUED .....</b>	<b>57</b>
<b>APPENDIX 5      SCHEDULE OF AMOUNTS DUE AND RECOVERED .....</b>	<b>59</b>
<b>APPENDIX 6      CONTRACT AUDIT REPORTS .....</b>	<b>60</b>
<b>APPENDIX 7      PEER REVIEW RESULTS .....</b>	<b>61</b>
<b>APPENDIX 8      ACRONYMS .....</b>	<b>62</b>
<b>APPENDIX 9      OIG HEADQUARTERS AND FIELD OFFICE CONTACTS AND LOCATIONS .....</b>	<b>64</b>
<b>APPENDIX 10     INDEX TO REPORTING REQUIREMENTS .....</b>	<b>67</b>

## 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 to September 30, 2010. 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 48 management reports (Appendix 3), 29 financial assistance grant reports (Appendix 4), and 546 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 \$77,597,951, of which \$24,976,746 was not supported by documentation. We recovered \$3,687,304 (Appendix 5) as a result of disallowed costs identified from current and previous audit

reports and from investigative efforts. We issued 10 reports identifying \$53,241,230 in funds put to better use. In addition, management agreed to deobligate \$25,613,545 in disaster grant assistance, which will result in funds put to better use. In the investigative area, we initiated 694 investigations and closed 600 investigations. Our investigations resulted in 198 arrests, 154 indictments, 115 convictions, and 89 personnel actions. Additionally, we reported \$6,508,342 million in collections resulting from fines and restitutions, administrative cost savings, and other recoveries.

We have a dual reporting responsibility both to Congress and to the department Secretary. During the reporting period, we continued our active engagement with Congress through extensive meetings, briefings, and dialogues. Members of Congress, their staff, 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 eight occasions during this reporting period. Testimony prepared for these hearings may be accessed through our website at [www.dhs.gov/oig](http://www.dhs.gov/oig).

## 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 the Department of Homeland Security (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 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 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 of 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
- Office of Policy
- Transportation Security Administration
- United States Citizenship and Immigration Services
- United States Coast Guard
- United States Customs and Border Protection
- United States Immigration and Customs Enforcement
- United States Secret Service



## Office of Inspector General Profile

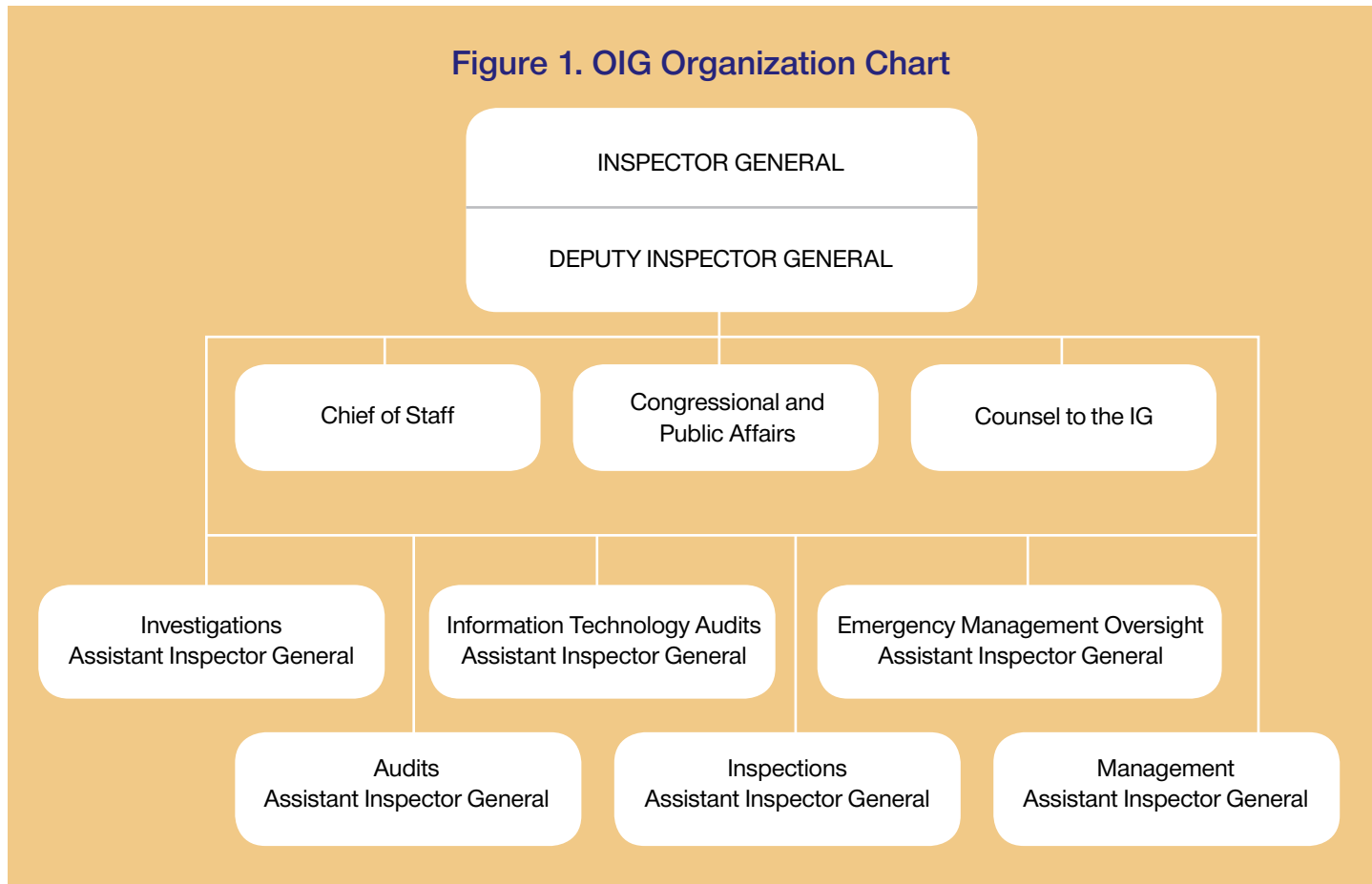
The *Homeland Security Act of 2002* provided for the establishment of an Office of Inspector General (OIG) in DHS by amendment to the *Inspector General Act of 1978* (5 USC App. 3, as amended). By this action, Congress and the administration ensured independent and objective audits, inspections, and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

The Inspector General is appointed by the President, subject to confirmation by the Senate, and reports directly to the Secretary of DHS and to Congress. The *Inspector General Act* ensures

the Inspector General’s independence. This independence enhances our ability to prevent and detect fraud, waste, and abuse, as well as to provide objective and credible reports to the Secretary and Congress regarding the economy, efficiency, and effectiveness of DHS’ programs and operations.

We were authorized 632 full-time employees during the reporting period. We consist of an Executive Office and eight functional components based in Washington, DC. We also have field offices throughout the country. Figure 1 illustrates the DHS OIG management team.

Figure 1. OIG Organization Chart





***The OIG consists of the following components:***

***The Executive Office*** consists of the Inspector General, the Deputy Inspector General, a Chief of Staff, and support staff. It provides executive leadership to the OIG.

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

***The Office of Counsel to the Inspector General*** 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* 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 whether 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)*** is responsible for providing an aggressive and ongoing audit effort designed to ensure that Disaster Relief Funds are being spent appropriately, while identifying fraud, waste, and abuse as early as possible. The office is an independent and objective means of keeping the Secretary of DHS, Congress, and other federal disaster relief agencies fully informed on problems and deficiencies relating to disaster operations and assistance programs, and progress regarding corrective actions. OIG focus is weighted heavily toward prevention, including reviewing internal controls, and monitoring and advising DHS and Federal Emergency Management Agency (FEMA) officials on contracts, grants, and purchase transactions before they are approved. This approach allows EMO to stay current on all disaster relief operations and provide on-the-spot advice on internal controls and precedent-setting decisions.

***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. Inspections 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, and inspection reports are released to DHS, Congress, and the public.

***The Office of Information Technology Audits (IT-A)*** conducts audits and evaluations of DHS' information management, cyber infrastructure, and systems integration activities. The office 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. The office also assesses DHS' information security program as mandated by the *Federal Information Security Management Act (FISMA)*. In addition, this office provides technical forensics assistance to OIG offices in support of OIG's fraud prevention and detection program.

***The Office of Investigations*** 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, the Office of Investigations provides oversight and monitors the investigative activity of DHS' various internal affairs offices. The office includes investigative staff working on gulf coast hurricane recovery operations.

***The Office of Management*** 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. The office also prepares the OIG's annual performance plans and semiannual reports to Congress.

# SUMMARY OF SIGNIFICANT OIG ACTIVITY



## DIRECTORATE FOR MANAGEMENT

### MANAGEMENT REPORTS

#### ***Independent Auditors' Report on Transportation Security Administration's FY 2009 Consolidated Balance Sheet as of September 30, 2009***

KPMG LLP, under contract with the OIG, audited the Transportation Security Administration's (TSA's) consolidated balance sheet as of September 30, 2009. KPMG issued a qualified opinion on the balance sheet owing to deficiencies regarding general property and equipment and future minimum lease payments.

The FY 2009 independent auditors' report also contains observations and recommendations related to internal control weaknesses that were considered significant deficiencies and were required to be reported. The four significant deficiencies in internal controls are presented below; the first three are considered material weaknesses.

#### **Significant Deficiencies**

1. Financial Management and Reporting
2. Property and Equipment
3. Other Liabilities
4. Information Technology Controls and Financial Systems Functionality

KPMG's tests of compliance with certain provisions of laws, regulations, contracts, and grants agreements identified two instances of noncompliance related to (1) the *Debt Collection Improvement Act of 1996* and (2) federal employment laws.

(OIG-10-78, April 2010, OA)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-78\\_Mar10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-78_Mar10.pdf)

#### ***Management Letter for the TSA's Consolidated Balance Sheet as of September 30, 2009***

KPMG LLP, under contract with the OIG, audited TSA's consolidated balance sheet as of September 30, 2009. KPMG also examined TSA's internal control over financial reporting and identified internal control weaknesses and other

operational matters, which resulted in a total of 11 financial management comment observations that did not reach the level required to be reported as significant deficiencies in our *Independent Auditors' Report on Transportation Security Administration's Consolidated Balance Sheet as of September 30, 2009*, dated March 23, 2010.

(OIG-10-79, April 2010, OA)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-79\\_Apr10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-79_Apr10.pdf)

#### ***DHS Needs to Address Challenges to Its Financial Systems Consolidation Initiative***

We reviewed DHS efforts to consolidate its component financial systems. Our objectives were to determine the progress DHS is making toward consolidating its systems and identify any challenges it faces to achieve its consolidation objectives. DHS is taking steps toward developing and implementing its systems consolidation program. The DHS Chief Financial Officer revised the Transformation and Systems Consolidation (TASC) initiative to acquire an integrated financial, acquisition, and asset management solution for DHS. However, DHS faces numerous challenges in implementing the TASC initiative. Specifically, DHS does not have the necessary planning documents in place and approved for this effort; total life cycle cost estimates are not inclusive of all project costs; and staffing projections have not been finalized. Additionally, DHS' Office of Chief Information Officer has had limited involvement with the overall initiative, which increases the risk that the DHS enterprise architecture and security requirements may not be incorporated into the new system.

(OIG-10-95, June 2010, IT-A)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-95\\_Jun10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-95_Jun10.pdf)

#### ***Stronger Security Controls Needed on Active Directory Systems***

The Department of Homeland Security uses Microsoft Windows Active Directory services to manage users, groups of users, computer systems, and services on its headquarters network. We reviewed the security of the Active Directory collection of resources and services used by components across the department through trusted connections. These resources and services

provide department-wide access to data that support department missions but require measures to ensure their confidentiality, integrity, and availability. The servers that host these resources must maintain the level of security mandated by department policy. Systems within the headquarters' enterprise Active Directory domain are not fully compliant with the department's security guidelines, and no mechanism is in place to ensure their level of security. These systems were added to the headquarters domain, from trusted components, before their security configurations were validated. Allowing systems with existing security vulnerabilities into the headquarters domain puts department data at risk of unauthorized access, removal, or destruction. Also, the department does not have a policy to verify the quality of security configuration on component systems that connect to headquarters. Interconnection security agreements are present for each connection between headquarters and components to secure shared services; however, neither the agreements nor other policy define specific security controls required for connecting systems. Stronger management and technical controls are needed on trusted systems to protect data provided by the department's enterprise-wide applications. We made three recommendations to address management and security issues to provide for a more secure Active Directory.  
(OIG-10-86, May 2010, IT-A)  
[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-86\\_May10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-86_May10.pdf)

***Management Oversight and Component Participation Are Necessary to Complete DHS' Human Resource Systems Consolidation Effort***

As required by the *E-Government Act of 2002* and the Office of Management and Budget's government-wide initiatives, in 2005 DHS Office of the Chief Human Capital Officer began to consolidate components' existing human resource information systems into five enterprise-wide solutions. Although DHS has made some progress in consolidating its human resource systems, as of February 2010, components have not migrated from their existing systems to all of the department's enterprise-wide systems. Additionally, DHS has not implemented adequate

performance metrics to track the status of the consolidation effort. Further, communication and system functionality must be improved to help facilitate the consolidation effort. Lastly, the certification and accreditation packages for DHS' enterprise-wide human resource systems do not include all required documents and security weaknesses are not being mitigated timely.

This report addresses the actions DHS has taken and progress made to consolidate components' existing human resource systems into enterprise-wide solutions. We made 11 recommendations addressing the need for the department to improve management oversight by implementing sufficient performance metrics, and enhancing communication and system functionality. Furthermore, the department must ensure that its human resource systems are certified and accredited according to applicable DHS policies and that identified deficiencies are addressed timely.  
(OIG-10-99, July 2010, IT-A)  
[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-99\\_Jul10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-99_Jul10.pdf)

***Information Technology Management Letter for the FY 2009 DHS Integrated Audit (Redacted)***

We contracted the independent public accounting firm KPMG LLP to perform a review of DHS' information technology (IT) general controls in support of the FY 2009 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 also performed technical security testing for key network and system devices, as well as testing over key financial application controls. KPMG noted that DHS took corrective action to address many prior years' IT control weaknesses. However, during FY 2009, 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 confidenti-

ality, integrity, and availability. In addition, these weaknesses negatively impact the internal controls over DHS' financial reporting and its operation, and KPMG considers them to collectively represent a material weakness under standards established by the American Institute of Certified Public Accountants.

(OIG-10-110, August 2010, IT-A)

[http://www.dhs.gov/woig/assets/mgmtrpts/OIGr\\_10-110\\_Aug10.pdf](http://www.dhs.gov/woig/assets/mgmtrpts/OIGr_10-110_Aug10.pdf)

### ***Management of DHS' Data Center Consolidation Initiative Needs Improvement***

We evaluated DHS' data center consolidation program. The overall objective of this audit was to evaluate the effectiveness of DHS' consolidation efforts to achieve its cost savings and efficiency goals.

The audit included reviews of DHS data center inventories, migration and spending plans, and prior audit reports. We reported that the department had not developed a complete inventory of the components' data centers. Additionally, the department should develop consolidated data center floor plans. Further, the department should update its enterprise-wide data center consolidation strategic plan to detail the process to decommission legacy component data centers and to conform to current government-wide efforts by the Office of Management and Budget to consolidate data centers.

We recommended that DHS (1) perform the necessary discovery and validation efforts to obtain accurate inventories of its data centers, hardware, and systems; and (2) review government-wide efforts as well as industry best practices for data center consolidations, and develop an updated comprehensive data center consolidation plan. DHS concurred with our second recommendation, but concurred with caveat to our first recommendation. Specifically, DHS stated that its three-phase approach for the planning of migration activities provides a sufficient amount of detail, minimizing inventory rework.

(OIG-10-120, September 2010, IT-A)

[http://www.dhs.gov/woig/assets/mgmtrpts/OIG\\_10-120\\_Sep10.pdf](http://www.dhs.gov/woig/assets/mgmtrpts/OIG_10-120_Sep10.pdf)

## **DIRECTORATE FOR NATIONAL PROTECTION AND PROGRAMS**

### **MANAGEMENT REPORTS**

#### ***U.S. Computer Emergency Readiness Team Makes Progress in Securing Federal Cyberspace, but Challenges Remain***

In 2003, the National Cyber Security Division created U.S. Computer Emergency Readiness Team (US-CERT) to protect the federal government network infrastructure by coordinating efforts to defend and respond to cyber attacks. US-CERT has made progress in implementing a cybersecurity program to assist federal agencies in protecting their information technology systems against threats. However, US-CERT does not have appropriate enforcement authority to ensure that agencies comply with its mitigation guidance concerning threats and vulnerabilities. Additionally, US-CERT does not have sufficient staff to perform its 24x7 operations and to analyze security information timely, and has not developed a strategic plan and must improve its information sharing efforts with federal agencies. Finally, US-CERT does not have the capability to monitor federal cyberspace in real time.

We recommended that US-CERT improve its management oversight by developing a strategic plan and approving policies and procedures to ensure that its analysis and warning program is effective. US-CERT must also ensure that it has sufficient staff to perform its missions, and should improve its information sharing and communications coordination efforts with the public. Finally, US-CERT needs to improve its situational awareness and identification capability by monitoring the federal cyber infrastructure for anomalies in real time.

(OIG-10-94, June 2010, IT-A)

[http://www.dhs.gov/woig/assets/mgmtrpts/OIG\\_10-94\\_Jun10.pdf](http://www.dhs.gov/woig/assets/mgmtrpts/OIG_10-94_Jun10.pdf)



National Cybersecurity and Communications Integration Center (NCCIC) Watch Floor.  
Source: US-CERT

### ***DHS Needs to Improve the Security Posture of Its Cybersecurity Program Systems***

Cyber threats pose a significant risk to economic and national security. In response to these threats, the President, legislators, experts, and others have characterized cybersecurity, or measures taken to protect a computer or computer system against unauthorized access or attack, as a pressing national security issue. This report identifies measures that can be taken to enhance the physical and logical controls on DHS' cybersecurity program systems to better protect the data collected, processed, and disseminated. Overall, DHS has implemented adequate physical security and logical access controls over the cybersecurity program systems used to collect, process, and disseminate cyber threat and warning information to the public and private sectors. However, a significant effort is needed to address existing security issues in order to implement a robust program that will enhance the cybersecurity posture of the federal government. We made 10 recommendations to address issues we identified regarding the timely deployment of system security patches to mitigate the risks to DHS' cybersecurity program systems, system security documentation, and adherence to departmental security policies and procedures. DHS management concurred with the recommendations and has already begun to take the actions to implement them.

(OIG-10-111, August 2010, IT-A)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-111\\_Aug10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-111_Aug10.pdf)

## **DIRECTORATE FOR SCIENCE AND TECHNOLOGY**

### **MANAGEMENT REPORTS**

#### ***Special Review of the Science and Technology Directorate's Contracts with a Small Business***

We assessed allegations that a Science and Technology (S&T) program manager violated regulations governing contract management by facilitating the development of his wife's research tool at National Research Laboratory (NRL) and providing her with S&T-funded software, including products funded by a Small Business Innovation Research contract. The NRL program manager used the tools to compete with the company that created the tools for federal research funding, according to the allegations, and the husband and wife used the threat of competition and other financial pressure to coerce the company into relinquishing rights to software it had developed. The program manager did not follow the department's policy to act with honesty and integrity and to avoid appearances of legal or ethical violations. We made four recommendations to resolve this situation and strengthen management oversight.

(OIG-10-103, July 2010, ISP)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-103\\_Jul10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-103_Jul10.pdf)

## **FEDERAL EMERGENCY MANAGEMENT AGENCY**

### **MANAGEMENT REPORTS**

#### ***NPSC Preparedness for Large-Scale Disasters***

Williams, Adley & Company, LLP, under a contract with the OIG, identified measures that FEMA can take to address the overall effectiveness of its National Processing Service Centers (NPSCs) to meet staffing requirements to manage the increased volumes of applications and assistance during large-scale disasters. The NPSCs are steadily improving in these areas,



but there are still systemic barriers that require management attention. These issues include the length of time it takes for temporary staff to obtain security clearances and the operational challenges of managing workspace, equipment, and personnel during surges in the workload. FEMA also needs a flexible and innovative approach for training inexperienced and temporary staff during these surges. Our recommendations included addressing the improvement of the quality and consistency of training and staff development, modifying interagency agreements to improve administration and security processes, and assessing the feasibility and cost-effectiveness of enhancing NPSC surge capacity.

(OIG-10-81, April 2010, EMO)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-81\\_Apr10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-81_Apr10.pdf)

#### ***Improving FEMA's Disaster Purchase Card Program***

The FEMA disaster purchase card program streamlines traditional federal procurement and payment processes by eliminating the need for numerous purchase orders and payments. When well controlled, it provides FEMA with a flexible and efficient way of quickly obtaining commercial goods and services through over-the-counter purchases, phone orders, mail/catalog orders, and Internet purchases. We concluded that, with more effective internal controls, FEMA could have prevented more than \$247,100 of improper purchases or detected them more quickly. An improper purchase is any purchase that should not have been made or that was made in an incorrect amount under statutory, contractual, or administrative requirements.

We recommended that FEMA improve its policies and procedures; take better advantage of preventive controls to minimize risk exposure; work with DHS and JP Morgan Chase to ensure that states and merchants do not tax purchases at the point of sale; establish a multifaceted, strategic approach to monitoring and oversight; and resolve issues with its transition to the General Services Administration SmartPay®2 and the Credit Card Transaction Management System.

(OIG-10-91, May 2010, EMO)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-91\\_May10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-91_May10.pdf)

#### ***Information Technology Management Letter for the FEMA Component of the FY 2009 DHS Integrated Audit***

We contracted the independent public accounting firm KPMG to perform the audit of FEMA Consolidated Balance Sheet and related statements as of September 30, 2009. As part of this review, KPMG noted certain matters involving internal control and other operational matters with respect to information technology 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 FEMA's financial processing environment and related IT infrastructure. KPMG noted that FEMA took corrective action to address many prior years' IT control weaknesses. However, during FY 2009, KPMG 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 the American Institute of Certified Public Accountants.

(OIG-10-92, May 2010, IT-A)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-92\\_May10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-92_May10.pdf)

#### ***FEMA's Disaster Assistance Improvement Plan***

FEMA faces challenges in implementing a "one-stop" disaster assistance application system because of the inability of partner agencies' systems to interface with DisasterAssistance.gov, and partner agencies' reluctance to provide funding to support the program. The agency was in the process of drafting internal control standard operating procedures but had not yet developed,

implemented, or strengthened controls. Further, the agency was in the process of coordinating with state, local, and voluntary organizations to integrate forms of assistance administered at the state and local levels.

Recommendations included implementing a funding model to ensure that DHS/FEMA funds the entire Disaster Assistance Improvement Plan (DAIP) program to include current contributions made by partner agencies; developing, implementing, and strengthening internal controls to prevent improper payments and other forms of fraud, waste, and abuse; and assisting pilot states with integration capabilities in order to interface with the DAIP.

(OIG-10-98, June 2010, EMO)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-98\\_Jun10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-98_Jun10.pdf)

***FEMA's Logistics Management Process for Responding to Catastrophic Disasters***

Logistics encompasses the procurement, supply, and maintenance of equipment and the provision of facilities; and the movement, evacuation, and supply/support of personnel and services. FEMA needs robust logistics capabilities, including an integrated approach to disaster logistics, to respond to catastrophic disasters. Despite progress made to date, the systems FEMA uses to support logistics operations do not communicate directly with those of key logistical partners; and some state and local jurisdictions' logistics capabilities were deficient because of staffing and budget shortfalls. We recommended that FEMA evaluate whether the Total Asset Visibility system being developed is on track to support logistics operations and work with its state partners to identify and overcome state and local logistical deficiencies.

(OIG-10-101, July 2010, EMO)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-101\\_Jul10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-101_Jul10.pdf)

***Federal Emergency Management Agency Mount Weather Emergency Operations Center Tenant Satisfaction Survey***

In response to concerns raised by Mount Weather Emergency Operations Center (MWEOC), tenants that were communicating with the OIG

conducted a tenant satisfaction survey related to the services provided by MWEOC. The objective of this tenant satisfaction survey was to measure tenant satisfaction levels with services provided by the MWEOC in Areas A and B. During our fieldwork we distributed and collected survey questionnaires and conducted interviews with MWEOC tenants, management, and employees. Additionally, we reviewed applicable documents provided by MWEOC management pertaining to customer service methodologies and procedures. The majority of the tenants in Areas A and B responded that they are either satisfied or very satisfied with the services provided by MWEOC in the following categories: environment, services, security, management staff, and features. Approximately one-third of the tenants in Area A and one-half of the tenants in Area B could not rate the cost of services provided by MWEOC.

(OIG-10-114, August 2010, OA)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-114\\_Aug10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-114_Aug10.pdf)

***FEMA's Management of Disaster Assistance Employee Deployment and Payroll Processes***

FEMA is authorized under the *Robert T. Stafford Disaster Relief and Emergency Assistance Act*, as amended, to temporarily expand its staff size to respond to major disasters and emergencies. Disaster assistance employees (DAEs) fulfill this role as excepted-service intermittent employees in disaster response and recovery operations. DAEs are critical in the agency's disaster operations, performing key program, technical, and administrative functions.

Improvements are needed in the DAE deployment and payroll processes in four areas. System updates are needed to the automated deployment system to allow managers to monitor and supervise disaster assistance employees. The time and attendance process is duplicative, and controls need to be strengthened to prevent errors. System vulnerabilities need to be eliminated to ensure accountability for disaster costs. Disaster assistance employee program guidance needs to be updated to include new program benefits policies to avoid conflicting guidance to managers. Our report provided four recommendations to improve

DAE deployment and payroll processes.  
(OIG-10-115, September 2010, EMO)  
[http://www.dhs.gov/xoig/assets/mgmtrpts/OIG\\_10-115\\_Sep10.pdf](http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_10-115_Sep10.pdf)

***The State of Maryland's Management of State Homeland Security Program and Urban Areas Security Initiative Grants Awarded During Fiscal Years 2005 through 2007***

Maryland received approximately \$40 million in State Homeland Security Program grants and \$33 million in Urban Areas Security Initiative grants awarded by FEMA during FYs 2005 through 2007. Regis & Associates, PC, under a contract with the OIG, conducted an audit of these grants to determine whether the state spent the funds strategically, effectively, and in compliance with laws, regulations, and guidance.

Overall, the State Administrative Agency did an efficient job of administering the program and distributing grant funds. Funding was linked to plans and core priorities identified by the Governor's Office of Homeland Security, and funds and resources were distributed based on those priorities. Reasonable methodologies were used for assessing threats and vulnerabilities and response capability. Grants were generally administered in compliance with applicable laws, regulations, and guidance.

However, improvements were needed in Maryland's management of the State Homeland Security Program grants regarding strategic planning and performance measurement, timely and accurate submission of financial status reports, monitoring of subgrantees, and support for expenditures submitted for reimbursement. Our five recommendations call for FEMA to require Maryland to initiate improvements which, if implemented, should help strengthen program management, performance, and oversight.  
(OIG-10-116, September 2010, OA)  
[http://www.dhs.gov/xoig/assets/mgmtrpts/OIG\\_10-116\\_Sep10.pdf](http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_10-116_Sep10.pdf)

***FEMA's Implementation of Recommendations from Top Officials 4***

House Report 110-862, Department of Homeland Security Appropriations Bill, 2009, requires that we review changes made by FEMA as a result of problems identified through Top Officials (TOPOFF) 4. Our review examined how FEMA incorporated corrective actions identified in TOPOFF 4 into National Level Exercise (NLE) 2009.

National-level exercises, formerly designated as TOPOFF exercises, are designed to reinforce the Nation's capability to prepare for, prevent, respond to, and recover from large-scale terrorist attacks or natural disasters. Exercise planners recognized that TOPOFF 4 and previous exercises focused almost exclusively on response and recovery operations. FEMA officials decided that it would be beneficial to alternate the type of threat each year to ensure that all homeland security mission areas were tested over time. Therefore, NLE 2009 emphasized mission areas that related to intelligence gathering and information sharing, which was a change in focus from TOPOFF 4. As a result, only 10 of the 54 corrective actions from TOPOFF 4 were relevant to NLE 2009.

To address deficiencies identified during national-level exercises, FEMA developed a centralized Corrective Action Program (CAP) where tracking and implementing corrective actions are the sole responsibility of each participating agency or department. Since FEMA has no enforcement authority to direct other departments and agencies to track and implement corrective actions, the overall effectiveness of the CAP system is reduced.

We recommended that FEMA develop reporting regulations for oversight of corrective action implementation. We accepted FEMA's suggestion to develop an alternative mechanism to strengthen corrective action progress in collaboration with the White House.  
(OIG-10-121, September 2010, ISP)  
[http://www.dhs.gov/xoig/assets/mgmtrpts/OIG\\_10-121\\_Sep10.pdf](http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_10-121_Sep10.pdf)

### ***FEMA's Preparedness for the Next Catastrophic Disaster – An Update***

We assessed FEMA's progress to improve preparedness for the next catastrophic disaster in 10 key preparedness areas. FEMA has made substantial progress in one of the key areas (Emergency Communications), moderate progress in seven areas (Overall Planning, Coordination and Support, Logistics, Evacuations, Housing, Acquisition Management, and Mitigation), and modest progress in two areas (Disaster Workforce and Mission Assignments). Concerns that are common to the critical components include the need for more effective coordination with state, local, and tribal governments; the need for IT systems that are updated and integrated agency-wide; insufficient experienced staff to handle the increasing workload; and funding that is not adequate to maintain initiatives, meet the costs of disasters, and recruit, train, and retain staff. Our 2008 report, *FEMA's Preparedness for the Next Catastrophic Disaster*, made three recommendations to (1) improve the agency's overall awareness of its readiness for a catastrophic disaster; (2) develop and sustain systems to track the progress of major programs, initiatives, and other activities; and (3) regularly share reports on the status of such activities with key stakeholders. We reiterated these recommendations, which remain open. (OIG-10-123, September 2010, EMO)  
[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-123\\_Sep10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-123_Sep10.pdf)

### **DISASTER ASSISTANCE GRANTS**

*The Robert T. Stafford Disaster Relief and Emergency Assistance Act* (Public Law 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 29 financial assistance grant reports during the period. Those reports disclosed questioned costs totaling \$77,543,638, of which \$24,922,433 was unsupported. A list of these reports, including questioned costs and unsupported costs, is provided in Appendix 4.

#### ***City of Buffalo, New York***

The city of Buffalo, NY, received a Public Assistance (PA) grant award of \$31 million from the New York State Emergency Management Office, a FEMA grantee, for damages resulting from severe storms in October 2006. The award provided 75% FEMA funding for debris removal, emergency protective measures, and repairs to city facilities and buildings. We reviewed costs totaling \$29.1 million claimed under the disaster. The city accounted for FEMA funds on a project-by-project basis according to federal regulations. However, the city's claim included \$4.3 million of charges that were excessive, unsupported, and ineligible. Also, the city did not maintain adequate documentation for the removal of hazardous trees and limbs. We recommended that the Regional Administrator, FEMA Region II, in coordination with the grantee, (1) disallow \$4.3 million of excessive, unsupported, and ineligible charges, and (2) instruct the city, for future disasters, to comply with FEMA guidance regarding the removal of hazardous trees and limbs. (DA-10-10, May 2010, EMO)  
[http://www.dhs.gov/xoig/assets/auditrpts/OIG\\_DA-10-10\\_May10.pdf](http://www.dhs.gov/xoig/assets/auditrpts/OIG_DA-10-10_May10.pdf)

#### ***City of Pass Christian, Mississippi***

The city of Pass Christian, MI, received a PA award of \$58.1 million from the Mississippi Emergency Management Agency (MEMA), a FEMA grantee, for damages related to Hurricane Katrina. The award provided 100% FEMA funding for debris removal, emergency protective measures, repairs to buildings and equipment, and other disaster-related activities. We reviewed costs totaling approximately \$6 million claimed under the award. The city's grant accounting system did not account for expenditures on a project-by-project basis as required by federal regulations, and the city was overpaid \$203,000 of FEMA funds under an emergency measures project. We also

concluded that \$547,000 of FEMA funding should be deobligated and \$31,000 of interest earned on advances should be remitted to FEMA. We recommended that the Regional Administrator, FEMA Region IV, in coordination with MEMA, (1) instruct the city to complete its efforts to account for expenditures on a project-by-project basis and to reimburse MEMA \$203,000 for the overpayment, (2) deobligate \$547,000 of FEMA funding not needed, and (3) require the city to remit \$31,000 in interest earned on advances. (DA-10-11, June 2010, EMO)

[http://www.dhs.gov/xoig/assets/auditreports/OIG\\_DA-10-11\\_Jun10.pdf](http://www.dhs.gov/xoig/assets/auditreports/OIG_DA-10-11_Jun10.pdf)

#### ***City of Hialeah, Florida***

The city of Hialeah, FL, received a PA grant award of \$11.7 million from the Florida Department of Community Affairs (DCA), a FEMA grantee, for damages resulting from Hurricane Wilma 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 \$11.3 million under the award. The city accounted for FEMA funds on a project-by-project basis according to federal regulations. However, the city's claim included \$2.5 million of costs that we questioned as unsupported, duplicate, ineligible, and excessive. We recommended that the Regional Administrator, FEMA Region IV, in coordination with DCA, disallow the \$2.5 million of questioned costs.

(DA-10-12, June 2010, EMO)

[http://www.dhs.gov/xoig/assets/auditreports/OIG\\_DA-10-12\\_Jun10.pdf](http://www.dhs.gov/xoig/assets/auditreports/OIG_DA-10-12_Jun10.pdf)

#### ***Hancock County School District, Mississippi***

The Hancock County School District, Mississippi, received a PA award of \$29 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 repair of buildings, equipment, and other facilities damaged as a result of the disaster. Our audit focused primarily on \$16.8 million claimed under six large projects. The district's grant accounting system did not account for expenditures on a project-by-project basis or

provide a means to readily trace project expenditures to source documents, as required by federal regulation. In addition, the district did not always comply with federal procurement procedures. Also, project charges included \$670,000 of questioned costs and \$35,000 of project funding that should be deobligated because the district received funding from another source to cover the authorized work. We recommended that the Regional Administrator, FEMA Region IV, in coordination with MEMA, (1) instruct the district to develop an accounting system that accounts for large projects on a project-by-project basis and to comply with federal procurement regulations when acquiring goods and services under the FEMA award, (2) deobligate duplicate funding totaling \$35,000, and (3) disallow \$59,000 of questioned costs.

(DA-10-14, July 2010, EMO)

[http://www.dhs.gov/xoig/assets/auditreports/OIG\\_DA-10-14\\_Jul10.pdf](http://www.dhs.gov/xoig/assets/auditreports/OIG_DA-10-14_Jul10.pdf)

#### ***South Mississippi Electric Power Association***

The South Mississippi Electric Power Association (SMEPA) received a PA award of \$11.9 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 SMEPA's power plants and transmission lines. Our audit focused primarily on \$2 million claimed under four large projects. SMEPA's grant accounting system did not account for expenditures on a project-by-project basis as required by federal regulation. In addition, SMEPA did not always comply with federal procurement procedures. SMEPA's claim also contained \$1.5 million of questionable costs resulting from ineligible equipment idle time and force account labor, and unreasonable costs billed by debris removal contractors. We recommended that the Regional Administrator, FEMA Region IV, in coordination with MEMA, (1) instruct SMEPA to develop an accounting system that accounts for large projects on a project-by-project basis and allows project expenditures to be traced to source documents, (2) instruct SMEPA to comply with federal procurement regulations when acquiring goods and services under the FEMA award, and

(3) disallow the \$1.5 million of questioned costs. (DA-10-15, July 2010, EMO)

[http://www.dhs.gov/xoig/assets/auditrpts/OIG\\_DA-10-15\\_Jul10.pdf](http://www.dhs.gov/xoig/assets/auditrpts/OIG_DA-10-15_Jul10.pdf)

#### ***Mississippi Coast Coliseum Commission***

The Mississippi Coast Coliseum Commission (coliseum) received a PA award of \$20.6 million from MEMA, a FEMA grantee, for damages related to Hurricane Katrina. The award provided 100% FEMA funding for debris removal, emergency protective measures, repairs to buildings and equipment, and other disaster-related activities. Our audit focused on \$12.3 million awarded under four large projects. The coliseum's grant accounting system did not account for expenditures on a project-by-project basis as required by federal regulations. In addition, the coliseum and MEMA did not comply with federal requirements and guidelines for improved projects, resulting in \$1.6 million of ineligible project funding and \$519,000 of ineligible project costs. We recommended that the Regional Administrator, FEMA Region IV, in coordination with MEMA, (1) instruct the coliseum to develop a system that fully accounts for costs on a project-by-project basis, (2) deobligate \$1.6 million of ineligible improved project funding, (3) disallow \$519,000 of ineligible project costs, and (4) deobligate any unneeded funding above the amount already recommended for deobligation by the review during project closeout.

(DA-10-16, August 2010, EMO)

[http://www.dhs.gov/xoig/assets/auditrpts/OIG\\_DA-10-16\\_Aug10.pdf](http://www.dhs.gov/xoig/assets/auditrpts/OIG_DA-10-16_Aug10.pdf)

#### ***Florida Department of Military Affairs***

The Florida Department of Military Affairs received awards totaling \$26 million from the Florida DCA, a FEMA grantee, for damages related to hurricanes Charley, Frances, and Jeanne that occurred in 2004. The award provided 100% FEMA funding for the first 72 hours and 90% funding thereafter for emergency protective measures and repair and restoration of public facilities. We reviewed costs totaling \$23.4 million awarded and claimed under six large projects. The department did not account for FEMA funds consistent with federal regulations. The

department's claim also included questionable costs totaling \$1.3 million (\$1.2 million FEMA share) resulting from excessive charges for administrative and mutual aid costs. We recommended that the Regional Administrator, FEMA Region IV, in coordination with DCA, (1) inform the department that it must comply with federal regulations when accounting for FEMA funds, and (2) disallow the \$1.3 million of questioned costs. (DA-10-18, September 2010, EMO)

[http://www.dhs.gov/xoig/assets/auditrpts/OIG\\_DA-10-18\\_Sep10.pdf](http://www.dhs.gov/xoig/assets/auditrpts/OIG_DA-10-18_Sep10.pdf)

#### ***City of Fort Lauderdale, Florida***

The city of Fort Lauderdale, FL, received PA awards totaling \$50.9 million from the Florida DCA, a FEMA grantee, for damages related to Hurricanes Katrina and Wilma. The awards provided 100% FEMA funding for emergency protective measures, debris removal activities, and repairs to recreation facilities and other public buildings. We reviewed costs totaling \$46.4 million under the two disasters, which consisted of \$9.2 million under Hurricane Katrina and \$37.2 million under Hurricane Wilma. The city accounted for FEMA funds on a project-by-project basis according to federal regulations for large projects. However, we questioned \$15.1 million of costs claimed, which resulted from excess funding for debris removal activities that had not been approved under the projects' scope of work; unreasonable contract charges; unsupported costs; small projects not implemented; excessive contract costs; and duplicate charges. The city also did not comply with federal procurement regulations and FEMA guidelines when awarding time-and-material contracts for debris removal activities. We recommended that the Regional Administrator, FEMA Region IV, in coordination with DCA (1) disallow the \$15.1 million of questioned costs, and (2) instruct the city, for future declarations, to comply with federal regulations and FEMA guidelines governing contracting practices. (DA-10-19, September 2010, EMO)

[http://www.dhs.gov/xoig/assets/auditrpts/OIG\\_DA-10-19\\_Sep10.pdf](http://www.dhs.gov/xoig/assets/auditrpts/OIG_DA-10-19_Sep10.pdf)

**Orleans Parish Criminal Sheriff's Office**

The Orleans Parish Criminal Sheriff's Office (OPCSO) received an award of \$6.3 million from the Louisiana Governor's Office of Homeland Security and Emergency Preparedness, a FEMA grantee, for work related to damages from Hurricane Katrina that occurred on August 29, 2005. The objective was to determine whether OPCSO expended and accounted for grant funds according to federal regulations and FEMA guidelines. OPCSO officials did not follow federal procurement standards in awarding and administering one of two agreements for catered meals. OPCSO's claim included \$2.5 million of costs that were ineligible. We recommended that FEMA (1) disallow \$1 million in unreasonable costs for employee meals, and (2) disallow \$1.5 million in duplicate funding for inmate meals.

(DD-10-08, March 2010, EMO)

[http://www.dhs.gov/xeig/assets/auditrrpts/OIG\\_DD-10-08\\_Mar10.pdf](http://www.dhs.gov/xeig/assets/auditrrpts/OIG_DD-10-08_Mar10.pdf)

**City of Bucyrus, Ohio**

We audited a hazard mitigation grant program (HMGP) for the city of Bucyrus, OH. The city was awarded \$2.6 million by the Ohio Emergency Management Agency, a FEMA grantee, to acquire residential properties (as many as 40 total) and to retrofit seven properties. Our objectives were to determine whether the city accounted for and expended FEMA funds according to federal regulations and FEMA guidelines, that the projects met FEMA eligibility requirements, and project management complied with applicable regulations and guidelines. As of July 2009, two of the three projects were complete and the city had claimed \$1.2 million in direct project costs. We audited \$1.2 million or 99% of these costs. The city did not always account for FEMA funds according to federal regulations and FEMA guidelines, and one project did not meet FEMA eligibility requirements because it was not cost-effective. As a result, we questioned \$40,398 (\$27,041 federal share) in unsupported labor costs and \$474,550 (\$345,297 federal share) as ineligible.

(DD-10-09, April 2010, EMO)

[http://www.dhs.gov/xeig/assets/auditrrpts/OIG\\_DD-10-09\\_Apr10.pdf](http://www.dhs.gov/xeig/assets/auditrrpts/OIG_DD-10-09_Apr10.pdf)

**Nebraska Public Power District, Columbus, Nebraska**

Nebraska Public Power District (NPPD), located in Columbus, NE, received a PA subgrant award of \$71.8 million from the Nebraska Emergency Management Agency (NEMA), a FEMA grantee, for damages caused by severe winter storms that occurred December 19, 2006, through January 1, 2007. NPPD accounted for and expended the majority of its FEMA grant funds (97% of the \$70.7 million audited) according to federal regulations and FEMA guidelines. However, NPPD's claim included ineligible costs for damages to private property, idle equipment, misclassified mutual aid work, duplicate mechanic charges, overstated labor, and easement and travel expenses. We recommended that FEMA disallow \$2,228,798 and request a waiver for the \$490,455 of misclassified mutual aid work.

(DD-10-10, June 2010, EMO)

[http://www.dhs.gov/xeig/assets/auditrrpts/OIG\\_DD-10-10\\_June10.pdf](http://www.dhs.gov/xeig/assets/auditrrpts/OIG_DD-10-10_June10.pdf)

**Recovery School District – Abramson High School**

The Recovery School District (RSD), in Baton Rouge, LA, received an award of \$37.2 million from the Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP), a FEMA grantee, for damages resulting from Hurricane Katrina. We audited \$17.6 million in funds advanced to the RSD for two project worksheets (PWs). The RSD did not account for and expend FEMA funds according to federal regulations and FEMA guidelines. RSD submitted a claim for \$859,487, of which GOHSEP allowed \$695,132, for approved demolition work at the site, and spent the remaining funds on work outside the scope of the two PWs. We recommended that the Regional Administrator, FEMA Region VI, disallow \$16.9 million for unauthorized work and deobligate the remaining award of \$19.6 million for work that was not performed.

(DD-10-14, July 2010, EMO)

[http://www.dhs.gov/xeig/assets/auditrrpts/OIG\\_DD-10-14\\_Jul10.pdf](http://www.dhs.gov/xeig/assets/auditrrpts/OIG_DD-10-14_Jul10.pdf)

**Louisiana State University Health Sciences Center**

Louisiana State University Health Sciences Center (LSUHSC), located in New Orleans, LA, received a PA subgrant award of \$93.3 million from the (GOHSEP), a FEMA grantee, for damages resulting from Hurricane Katrina. We audited \$56.2 million in funds advanced to the Center for nine PWs. LSUHSC did account for and expend FEMA funds according to federal regulations and FEMA guidelines; however, the Center's claimed costs totaled \$3,044,234 less than the total amounts obligated on the PWs. We also identified three emergency work projects that have the same scope of work as permanent work projects approved for the same buildings. We recommended that FEMA deobligate \$3,044,234 in federal funds and put them to better use and to identify and deobligate funding for permanent work that is identical to the scope of work in emergency protective measure projects for the same facilities. (DD-10-15, July 2010, EMO)

[http://www.dhs.gov/xoig/assets/auditreports/OIG\\_DD-10-15\\_Jul10.pdf](http://www.dhs.gov/xoig/assets/auditreports/OIG_DD-10-15_Jul10.pdf)

**Lamar University**

Lamar University received an award of \$25.9 million from the Texas Division of Emergency Management, a FEMA grantee, for damages caused by Hurricane Rita in September 2005. The objective of the audit was to determine whether the university accounted for and expended FEMA grant funds according to federal regulations and FEMA guidelines. The university did not account for and expend all FEMA grant funds according to federal regulations and FEMA guidelines. The university's claim of \$26.9 million (FEMA share 100%) in questioned costs included unsupported costs, unused federal funds, and ineligible costs. We recommended that the Regional Administrator, FEMA Region VI, (1) disallow unsupported costs of \$22.8 million, (2) monitor the state's progress in assisting the university in revising and finalizing its claim, (3) disallow \$2.7 million of ineligible cost overruns, (4) deobligate unused federal funds totaling \$1.4 million, and (5) disallow the \$85,993 of ineligible costs not related to the disaster.

(DD-10-16, August 2010, EMO)

[http://www.dhs.gov/xoig/assets/auditreports/OIG\\_DD-10-16\\_Aug10.pdf](http://www.dhs.gov/xoig/assets/auditreports/OIG_DD-10-16_Aug10.pdf)

**Louisiana Department of Health and Hospitals**

The Louisiana Department of Health and Hospitals (LDHH), a statewide agency headquartered in Baton Rouge, LA, received a PA subgrant award of \$68.78 million from the Louisiana GOHSEP, a FEMA grantee, for Category B work (emergency protective measures) resulting from Hurricane Katrina. As of February 2010, FEMA had written and approved two sets of PWs totaling \$44.91 million for substantially the same work, but had not reconciled the two sets of PWs. As a result, our audit scope was limited because we could not allocate LDHH's claimed costs to approved work and, therefore, could not determine whether LDHH accounted for and expended FEMA grant funds according to federal regulations and FEMA guidelines. We recommended that FEMA deobligate \$22,569,311 in federal funds and put them to better use; work with GOHSEP and LDHH to develop a plan to reconcile costs claimed for all Category B work and close out the applicable PWs; and ensure that GOHSEP improves its procedures for assisting its subgrantees to account for eligible costs. (DD-10-17, September 2010, EMO)

[http://www.dhs.gov/xoig/assets/auditreports/OIG\\_DD-10-17\\_Sep10.pdf](http://www.dhs.gov/xoig/assets/auditreports/OIG_DD-10-17_Sep10.pdf)

**County of Los Angeles, California**

The County of Los Angeles, CA received a PA subgrant award of \$10.9 million from the California Office of Emergency Services, a FEMA grantee, for debris removal, emergency protective measures, and permanent repairs to facilities damaged by severe storms in February 2005. FEMA provided 75% federal funding for 36 large and 3 small projects. We audited 12 completed large projects with a total award of \$3.8 million and noted that as of January 23, 2009, the County had been reimbursed \$3.5 million of the \$3.8 million and plans to claim an additional \$3 million in cost overruns. We questioned \$2.46 million in amounts to be claimed by the Department and identified \$271,878 in funds that were no longer needed for project execution. We recommended that FEMA (1) disallow \$2.34 million in ineligible project cost overruns, (2) disallow \$87,295 in overstated straight-time labor fringe benefits costs, and (3) disallow \$35,209 in costs relating



to a federal-aid road. We also made two other recommendations – one relating to the establishment of controls that prevent subgrantees from claiming costs that were previously denied by FEMA, and one that FEMA reduce funding on six projects by \$271,878 since the funds are no longer needed.

(DS-10-07, April 2010, EMO)

[http://www.dhs.gov/xoig/assets/auditrrpts/OIG\\_DS-10-07\\_Apr10.pdf](http://www.dhs.gov/xoig/assets/auditrrpts/OIG_DS-10-07_Apr10.pdf)

#### ***FEMA's Practices for Evaluating Insurance Coverage for Disaster Damage and Determining Project Eligibility and Costs***

During our audit of *Gulf Coast Recovery: FEMA's Management of the Hazard Mitigation Component of the Public Assistance Program* (OIG-10-28, December 10, 2009), we identified reportable conditions outside the scope of that audit. We employed audit procedures related to these conditions to determine whether FEMA effectively managed selected areas of the PA program across the gulf coast region in the aftermath of Hurricanes Wilma and Rita. We reported that FEMA needs to strengthen procedures and processes for (1) reviewing insurance coverage, recording insurance recoveries, and maintaining related supporting documentation (Louisiana and Texas); (2) applying the cost estimating format (CEF) methodology and maintaining documentation that supports the assumptions used in CEF calculations (Louisiana); and (3) maintaining documentation to support project eligibility and funding determinations (Texas). We made five recommendations that address these conditions and questioned \$21.1 million related to unverified insurance allocations (\$15.9 million), overstated project costs (\$3.9 million), and ineligible costs (\$1.3 million).

(DS-10-08, June 2010, EMO)

[http://www.dhs.gov/xoig/assets/auditrrpts/OIG\\_DS-10-08\\_Jun10.pdf](http://www.dhs.gov/xoig/assets/auditrrpts/OIG_DS-10-08_Jun10.pdf)

#### ***City of Napa, California***

The city of Napa, CA, received a PA subgrant award of \$4 million from the California Emergency Management Agency (Cal EMA), a FEMA grantee, for emergency protective measures and permanent repairs to facilities damaged by severe

storms in December 2005. FEMA provided 75% federal funding for 9 large and 23 small projects. We audited nine large projects with a total award of \$3.6 million. We identified \$386,617 in funding that the city no longer needed for two projects. We also reported that the city should submit quarterly progress reports to Cal EMA and improve its accounting for disaster-related costs. Additionally, estimated costs for one project in the design phase had increased significantly, and the changes in the scope of work were not eligible for FEMA funding. We recommended that FEMA (1) deobligate \$386,617 in disaster funds, (2) require Cal EMA to adhere to the monitoring and program performance reporting requirements, (3) require Cal EMA to ensure that the city improves record keeping procedures and supports disaster grant costs with properly maintained documentation, and (4) inform CalEMA that \$656,078 in improvements required by another federal agency are not eligible for PA funding.

(DS-10-09, July 2010, EMO)

[http://www.dhs.gov/xoig/assets/auditrrpts/OIG\\_DS-10-09\\_Jul10.pdf](http://www.dhs.gov/xoig/assets/auditrrpts/OIG_DS-10-09_Jul10.pdf)

#### ***City of Glendale, California***

The city of Glendale, CA, received a PA subgrant award of \$4.3 million from Cal EMA, a FEMA grantee, for emergency protective measures and permanent repairs to facilities damaged by severe storms in December 2004 and January 2005. FEMA provided 75% federal funding for 10 large projects and 13 small projects. We audited all 10 large projects with a total award of \$4.2 million. We identified \$146,257 in ineligible project charges and \$124,082 in unsupported costs and duplicative entries. We also identified \$19,748 in charges covered by FEMA's statutory administrative allowance. We recommended that (1) Cal EMA disallow \$290,087 of questioned costs that the city identified as claimable costs, and (2) FEMA and Cal EMA ensure that costs reported by the city for selected projects are valid and supported by adequate documentation.

(DS-10-10, September 2010, EMO)

[http://www.dhs.gov/xoig/assets/auditrrpts/OIG\\_DS-10-10\\_Sep10.pdf](http://www.dhs.gov/xoig/assets/auditrrpts/OIG_DS-10-10_Sep10.pdf)

***City of Rancho Palos Verdes, California***

The city of Rancho Palos Verdes, CA, received a PA subgrant award of \$964,891 from Cal EMA, a FEMA grantee, for debris removal, emergency protective measures, and repairs to utilities and other facilities damaged by severe storms from December 2004 to January 2005. FEMA provided 75% federal funding for two large projects and four small projects. We audited the two large projects and two small projects with a total award of \$938,762. We identified \$559,699 in ineligible project charges that were the responsibility of the Federal Highway Administration and \$357,173 in costs that were not related to disaster damage, but rather were due to deferred maintenance. We recommended that FEMA, in coordination with Cal EMA, collect a total of \$916,872 in ineligible and nondisaster costs we questioned in the report. (DS-10-11, September 2010, EMO)  
[http://www.dhs.gov/xoig/assets/auditrpts/OIG\\_DS-10-11\\_Sep10.pdf](http://www.dhs.gov/xoig/assets/auditrpts/OIG_DS-10-11_Sep10.pdf)

**INVESTIGATIONS*****Former Police Officer Guilty of FEMA Grant Fraud***

As the result of our investigation, a recently retired Florida police officer and former Officer of the Year was found guilty on two counts of money laundering following a federal jury trial. She was found guilty of laundering more than \$200,000 of FEMA grant funds for her personal use over a 4-year period. The retired officer was remanded directly into federal custody until sentencing in November. We located and seized the misused FEMA funds.

***Disaster Benefit Applicant Sentenced to 1 Year in Prison***

A Disaster Benefit applicant was sentenced to 12 months' incarceration, 3 years' probation, and ordered to pay restitution of \$50,300 related to her guilty plea to violation of conspiracy in the United States District Court. Our investigation determined that the applicant conspired with her ex-husband and received more than \$100,000 in FEMA benefits for Hurricane Katrina, and they further conspired and defrauded the U.S. government by more than \$72,000 for five disaster-related claims by utilizing multiple Social Security

numbers not belonging to them and by submitting bogus rent receipts for housing assistance payments.

***\$560,500 Cost Savings to Firefighters Grant Program***

A joint investigation we conducted with the FEMA Assistance to Firefighters Grant Program (AFG) reported that, as a direct result of an ongoing DHS-OIG grant fraud investigation, the AFG office has rejected funding on five AFG applications in a local jurisdiction. The total amount of the five FEMA-AFG rejections equals \$560,500. This amount is a cost savings resulting from our investigative efforts.

***Subject Sentenced in Fraud Investigation over \$100,000******(Update 10/01/09 – 3/31/10 SAR)***

A FEMA Disaster Benefit recipient who pleaded guilty to a charge of theft of government funds was sentenced to 3 years' probation and ordered to pay \$105,000 in restitution to a Road Home Program, and \$14,858 in restitution to FEMA. Our joint investigation with the Department of Housing and Urban Development OIG and the Federal Bureau of Investigation (FBI) revealed that during Hurricane Katrina, the individual resided in his primary residence outside the disaster zone. In 2006, he applied for funds from a Road Home Program, claiming that a second home he owned, located within the disaster area, was his primary residence at the time of the storm. He admitted that as a result of his fraudulent application, he received approximately \$105,000 in Road Home Program funds to which he was not entitled.

***Last Defendant Sentenced in "Operation Stolen Bayou"***

The last of eight defendants in "Operation Stolen Bayou" was sentenced to 57 months' confinement, 3 years' probation, \$300 fine, and restitution of \$299,351 following his conviction for conspiracy and removing/altering motor vehicle identification numbers (VIN). The combined total ordered restitution in this investigation for all eight felons was \$2,055,892. The case was investigated by the FBI, state and local police, the DHS OIG, the United States Marshals Service, and the state's

Department of Public Safety and Corrections. This joint investigation was initiated in September 2006 upon information received from state and local investigators from a number of agencies regarding the theft of vehicles and the theft of VINs stemming from vehicles lost, stolen, or damaged during Hurricane Katrina. Eighty-five names were fraudulently submitted to the Internal Revenue Service and FEMA in an effort to receive potential government benefits, and the investigation linked the defendant to the conspiracy of removing/altering motor VINs.

#### ***Individual Defrauded FEMA of \$33,734***

Our office was notified by FEMA of an individual who made 23 separate claims using variations of his name, Social Security number, and other identification. Our investigation revealed that he filed 23 separate claims from four separate hurricane disasters and received \$33,734 by fraudulently claiming to be a resident of the disaster areas and using false personal identifiers. When we located and arrested the subject, he was already in a local jail pending other charges for identity theft. The subject entered a guilty plea and was sentenced to 33 months' incarceration, 3 years' probation, and ordered to pay full restitution to FEMA.

#### ***FEMA Employee Conspired With Relative to Steal \$721,212 of Disaster Funds***

We conducted a joint investigation with the FBI of a FEMA employee that subsequently led the indictment and arrest of the employee and a relative for conspiracy to defraud FEMA. The FEMA employee was hired to work in a FEMA Individual Assistance program, where she manipulated the applications of actual disaster victims to increase the amount of disaster funds they were awarded. The employee then routed the additional funds from the disaster victims into the bank account of her relative. FEMA fired the employee. The former employee and her relative both entered guilty pleas in federal court. The former employee was sentenced to 82 months in prison, 5 years' probation, and ordered to jointly pay with her relative \$721,212 restitution to FEMA. The relative was sentenced to serve 114 months' incarceration, 5 years' probation, and to jointly pay restitution to FEMA.

#### ***Individual Claims 20 False Addresses to Receive \$41,216 From FEMA***

We investigated an individual who used false names and Social Security numbers to file 20 disaster claims with FEMA, claiming to have been a resident of New Orleans when Hurricane Katrina struck. As a result of the false claims, she received 18 FEMA checks totaling \$41,216. She entered a guilty plea and was sentenced to 28 months' confinement, 3 years' probation, and ordered to pay \$41,216 restitution to FEMA.

## **FEDERAL LAW ENFORCEMENT TRAINING CENTER**

### **MANAGEMENT REPORTS**

#### ***Information Technology Management Letter for the FY 2009 Federal Law Enforcement Training Center Financial Statement Audit***

We contracted the independent public accounting firm KPMG to perform the audit of Federal Law Enforcement Training Center (FLETC) consolidated balance sheet in support of DHS' financial statement audit as of September 30, 2009. As part of this review, KPMG noted certain matters involving internal control and other operational matters with respect to information technology 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 FLETC's financial processing environment and related IT infrastructure. KPMG noted that FLETC took corrective action to address many prior years of IT control weaknesses. However, during FY 2009, KPMG 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 over 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 considers them to collectively represent a material weakness under standards established by the American Institute of Certified Public Accountants.

(OIG-10-83, April 2010, IT-A)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-83\\_Apr10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-83_Apr10.pdf)

## OFFICE FOR CIVIL RIGHTS AND CIVIL LIBERTIES

We received 99 civil rights and civil liberties complaints from April 1 through September 30, 2010. Of those, we opened 12 investigations and referred 87 complaints to the Office for Civil Rights and Civil Liberties. Currently, there are no complaints under review for disposition.

## OFFICE OF COUNTERNARCOTICS ENFORCEMENT

### MANAGEMENT REPORTS

#### *The Responsibilities of the Office of Counternarcotics Enforcement*

We reviewed how the Office of Counternarcotics Enforcement (CNE), part of the Office of the Secretary, fulfills its statutory mandates. We determined that CNE has faced various challenges in coordinating departmental policy, analyzing component counternarcotics budgets, and serving as a DHS representative across agencies and levels of government. We recommended various improvements to help CNE become the key player in policy coordination envisioned in the statute. We also concluded that CNE is not the most effective office to coordinate counternarcotics operations or to track and sever connections between drug trafficking and terrorism. Our recommendations included action to effect statutory change that would relieve CNE of these two responsibilities. CNE concurred with six of our nine recommendations.

(OIG-10-80, April 2010, ISP)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-80\\_Apr10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-80_Apr10.pdf)

## TRANSPORTATION SECURITY ADMINISTRATION

### MANAGEMENT REPORTS

#### *Information Technology Management Letter for the FY 2009 Transportation Security Administration Financial Integrated Audit*

We contracted the independent public accounting firm KPMG to perform the audit of TSA's consolidated balance sheet in support for DHS' financial statement audit as of September 30, 2009. As part of this review, KPMG noted certain matters involving internal control and other operational matters with respect to information technology 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 noted that TSA took corrective action to address many prior years' IT control weaknesses. However, during FY 2009, KPMG 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 TSA's Finance Center (FINCEN). 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 considers them to collectively represent a significant deficiency under standards established by the American Institute of Certified Public Accountants.

(OIG-10-82, April 2010, IT-A)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-82\\_Apr10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-82_Apr10.pdf)

### ***Evaluation of Screening of Air Cargo Transported on Passenger Aircraft***

TSA could improve its efforts to ensure air carriers and certified cargo screening facilities are effectively screening cargo transported on passenger aircraft. The agency's inspection process has not been effective in ensuring that screening personnel are properly trained or applying the procedures. The agency has only recently begun performing covert tests in this area to prevent poor practices and complacency. The details of our testing are classified; however, we shared the results with the agency.

We made five recommendations that will improve the agency's screening and security measures to prevent the introduction of explosives into air cargo shipped on passenger aircraft. The agency concurred with two recommendations and partially concurred with three recommendations. (OIG-10-119, September 2010, OA)

[http://www.dhs.gov/woig/assets/mgmttrpts/OIG\\_10-119\\_Sep10.pdf](http://www.dhs.gov/woig/assets/mgmttrpts/OIG_10-119_Sep10.pdf)

### **INVESTIGATIONS**

#### ***\$232,238 in "Disallowable Costs" Returned to TSA***

In July of this year, we were notified by Forensic Accountants, Office of Chief Counsel (OCC), TSA, that TSA OCC received a check from a major government contractor in the amount of \$232,328 as payment for "disallowable costs." The contracting corporation had previously provided employee recruitment and training services to TSA. As a result of our investigation of allegations of excess billing, the company executed a Settlement Agreement in the amount of \$5,648,293 with the Department of Justice, Civil Division, Commercial Litigation Branch. A provision in the Settlement Agreement required the company to identify and reimburse TSA for those contract training costs previously invoiced to TSA that were now disallowable under terms of the Settlement Agreement.

## **UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES**

### **MANAGEMENT REPORTS**

#### ***Information Technology Management Letter for the FY 2009 U.S. Citizenship and Immigration Services Financial Statement Audit***

We contracted the independent public accounting firm KPMG to perform the audit of the United States Citizenship and Immigration Services (USCIS) Consolidated Balance Sheet and related statements as of September 30, 2009. As part of this review, KPMG noted certain matters involving internal control and other operational matters with respect to information technology 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 USCIS' financial processing environment and related IT infrastructure. KPMG noted that USCIS took corrective action to address many prior years' IT control weaknesses. However, during FY 2009, KPMG continued to find IT general control weaknesses at USCIS. The most significant weaknesses from a financial statement audit perspective related to controls over the Federal Financial Management System (FFMS) and weaknesses in physical security and security awareness. 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 USCIS' financial reporting and its operation, and KPMG considers them to collectively represent a material weakness under standards established by the American Institute of Certified Public Accountants.

(OIG-10-93, June 2010, IT-A)

[http://www.dhs.gov/woig/assets/mgmttrpts/OIG\\_10-93\\_Jun10.pdf](http://www.dhs.gov/woig/assets/mgmttrpts/OIG_10-93_Jun10.pdf)

### ***Efforts to Detect and Deter Fraud Committed by Immigration Services Officers***

We reviewed actions that USCIS has taken to deter fraud and misconduct by Immigration Services Officers who process requests for immigration benefits and engage in improper activities. We determined that the USCIS Office of Security and Integrity has learned from previous cases of misconduct and has expanded training on ethical expectations. After discussions with Immigration Service Officers, field managers, and headquarters staff, we identified further areas for greater efficiency, including the reiteration of the requirement that employees must report alleged misconduct, as well as ways to better deter misconduct. USCIS concurred with all six of the report's recommendations.

(OIG-10-118, September 2010, ISP)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-118\\_Sep10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-118_Sep10.pdf)

## **INVESTIGATIONS**

### ***USCIS Adjudication Officer Pleads Guilty to Solicitation of Sexual Favors***

A former USCIS District Adjudication Officer pleaded guilty in state court to bribery, coercion, and sexual misconduct. An investigation we conducted with the local District Attorney Detective Bureau determined that the USCIS Adjudication Officer solicited and received sexual favors from an applicant seeking immigration benefits by causing her to fear that if she did not comply with his request her benefit application would be denied. In his plea, the USCIS employee admitted to calling the applicant whose application he was reviewing and asking her to meet him in his car outside the USCIS office. He then coerced her to perform a sexual favor in return for assistance in obtaining a green card. The employee was terminated by USCIS and was sentenced in state court to 54 months' confinement.

### ***Conviction Obtained in Immigration Fraud Investigation***

As a part of our continuing investigations related to the case of a former Supervisory Adjudications Officer, USCIS, in which numerous individuals conspired with the USCIS employee and his co-conspirator to fraudulently obtain immigration benefits, we and the FBI arrested an additional civilian participant. She was one of the subjects indicted as a result of her actions as a document broker illegally obtaining genuine immigration documents. She subsequently pleaded guilty to fraud and misuse of immigration documents and abetting. Sentencing has been scheduled for later this year.

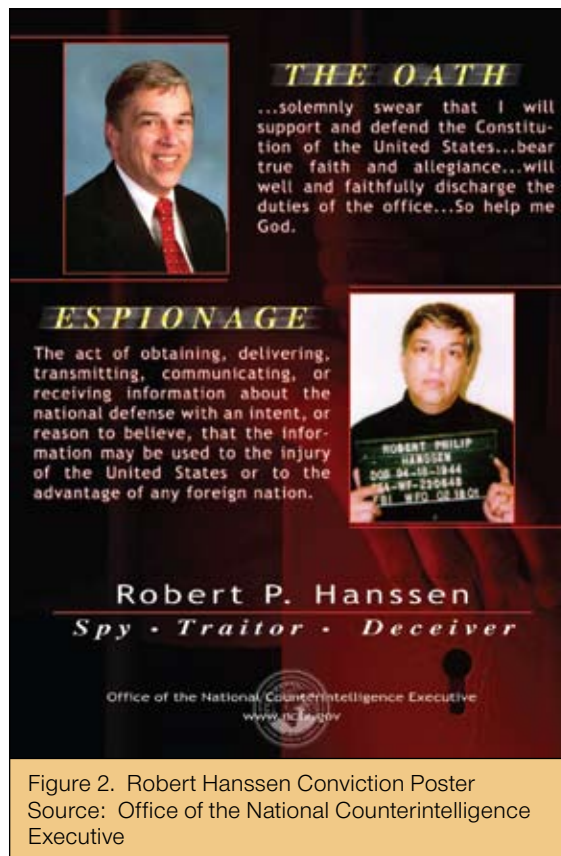


Figure 2. Robert Hanssen Conviction Poster  
Source: Office of the National Counterintelligence Executive

## UNITED STATES COAST GUARD

### MANAGEMENT REPORTS

#### *Information Technology Management Letter for the United States Coast Guard Component of the FY 2009 DHS Financial Statement Audit*

We contracted the independent public accounting firm KPMG to perform the audit of the United States Coast Guard (USCG) consolidated balance sheet in support of DHS' financial statement audit as of September 30, 2009. As part of this review, KPMG noted certain matters involving internal control and other operational matters with respect to information technology 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 noted that USCG took corrective action to address many prior years' IT control weaknesses. However, during FY 2009, KPMG 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 FINCEN. 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 considers them to collectively represent a material weakness at the department level under standards established by the American Institute of Certified Public Accountants.

(OIG-10-77, April 2010, IT-A)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-77\\_Apr10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-77_Apr10.pdf)

#### *Coast Guard's Blueprint for Acquisition Reform Needs Improved Oversight*

The Coast Guard began realigning its acquisition function in 2007 in response to issues reported by our office and the Government Account-

ability Office. The Coast Guard's Blueprint for Acquisition Reform sets forth objectives and specific action items for improving its acquisition function and contracting capabilities. We conducted this audit to determine the progress the Coast Guard has made in implementing its Blueprint. We concluded that the Coast Guard could improve its Blueprint implementation oversight by (1) establishing a method to measure outcomes of completed Blueprint action items and (2) prioritizing the action items. We recommended that the Coast Guard establish a more effective methodology for assessing Blueprint implementation progress, establish priorities among the Blueprint's action items, and evaluate and take corrective actions to mitigate the effect of delayed completion of action items.

(OIG-10-84, April 2010, OA)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-84\\_Apr10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-84_Apr10.pdf)

#### *The Coast Guard's Boat Crew Communications Systems Is Unreliable*

We conducted this work as part of our audit to determine whether the current Maritime Safety and Security Team (MSST) program and structure is the best approach for the Coast Guard to accomplish its maritime law enforcement and homeland security missions. We found issues with the current small boat crew communications system, and determined that the system is unreliable and poses a safety risk to MSST boat



MSST boat crew demonstrating the high-speed maneuverability of a 25-foot small boat in the Port of Anchorage, Alaska.  
Source: Coast Guard

crews, as well as other Coast Guard crews aboard the Rescue Boat-Small. Interim solutions to technical problems that cause the communication headsets to abruptly lose power have not been adequate, and it could take up to 10 years for new and improved replacement equipment to be provided. Until this issue is addressed, MSST operational readiness and the safety of crew members and the boating public may be at risk. We recommended that the Coast Guard develop an interim solution to immediately address problems with the system to reduce the risk of crew fatalities resulting from ineffective communication during maritime operations.

(OIG-10-85, May 2010, OA)

[http://www.dhs.gov/xoig/assets/mgmtrpts/OIG\\_10-85\\_May10.pdf](http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_10-85_May10.pdf)

#### ***The Coast Guard's Maritime and Safety Security Team Program***

The *Maritime Transportation Security Act of 2002* created Maritime Safety and Security Teams to function as part of the DHS layered strategy for protecting the Nation's seaports and waterways. The Coast Guard currently has 12 teams located across the United States that have provided support for events such as the G-20 Summit, national political conventions, the Presidential inauguration, the Super Bowl, military outloads, major maritime events, and international piracy



A boat crew from Coast Guard Maritime Safety and Security Team 91111 demonstrates the high-speed maneuverability of a 25-foot small boat at the Port of Anchorage.

Source: Coast Guard

missions. We conducted this audit to determine if the Coast Guard's Maritime Safety and Security Team program optimally meets the Coast Guard's maritime law enforcement and homeland security mission requirements in the current threat environment, and we reviewed the initial justification for establishing the program. We determined that the Coast Guard does not know if this program is the optimal vehicle to conduct its maritime law enforcement and homeland security missions in the current threat environment because it has not conducted a comprehensive analysis to validate that the current structure of this program is the best approach for achieving the program's goals. We recommended that the Coast Guard conduct a comprehensive analysis of the program, including determining optimal staffing levels, alignment of equipment with mission requirements, and the return on investment and opportunity costs associated with the current Maritime Safety and Security Team structure.

(OIG-10-89, May 2010, OA)

[http://www.dhs.gov/xoig/assets/mgmtrpts/OIG\\_10-89\\_May10.pdf](http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_10-89_May10.pdf)

#### ***Funding Plan for the United States Coast Guard Museum***

Enacted on August 9, 2004, the *Coast Guard and Maritime Transportation Act of 2004* (P.L. 108-293), authorized the establishment of a Coast Guard Museum in New London, CT. This act requires that, prior to the establishment of the museum, the Coast Guard submit a funding plan for the construction, operation, and maintenance of the museum. Further, according to this act, the DHS Inspector General is to certify that the estimates in the plan are reasonable and realistic before the plan is submitted to Congress. We conducted this audit to determine whether cost estimates in the Coast Guard's Funding Plan for the Coast Guard Museum to construct and operate the National Coast Guard Museum are reasonable and realistic. We determined that the estimated operating costs appear both reasonable and realistic; however, our conclusion relies on the presumption that the National Coast Guard Museum Association will raise sufficient funds to construct a facility capable of achieving the



museum's operational objectives. If the National Coast Guard Museum Association fails to raise sufficient funds, the museum may not achieve its budgeted revenues and federal funding requirements may increase. We made two recommendations to the Coast Guard, which are designed to ensure a continued realistic capital budget and operating forecast for the Coast Guard Museum. (OIG-10-105, August 2010, OA)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-105\\_Aug10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-105_Aug10.pdf)

#### ***Annual Review of the United States Coast Guard's Mission Performance (FY2009)***

The *Homeland Security Act of 2002* requires the DHS OIG to conduct an annual review of the U.S. Coast Guard's mission performance. We reviewed the Coast Guard'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 2009. We determined that the Coast Guard dedicated more resource hours to homeland security missions than to non-homeland security missions for the eighth consecutive year. The Coast Guard met more non-homeland security performance measures than homeland security performance measures, and expects to spend more on homeland security missions in FY 2010.

(OIG-10-106, August 2010, OA)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-106\\_Aug10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-106_Aug10.pdf)

#### ***Recommendations to Improve the Coast Guard's System for Adjudicating Suspension and Revocation Matters***

While assessing the validity of a former Administrative Law Judge's allegations of bias and misconduct in the Coast Guard's Administrative Law Judge program, we became familiar with the Administrative Law Judge (ALJ) program and the Coast Guard's suspension and revocation administrative proceedings, and noted programmatic issues not directly related to the allegations that warranted management's attention. The ALJ program needs to review and update certain policies and procedures regarding the training,

investigation, and discipline of Administrative Law Judges. The Coast Guard should also train and provide adequate legal support to its investigating officers. Commandant Decisions on Appeal need to be issued more timely and be more accessible to the public. Finally, the Coast Guard should establish guidelines governing interaction between staff handling prosecutorial and adjudicative functions. We made 11 recommendations to address these issues and to improve the effectiveness, integrity, and efficiency of the both the ALJ program and suspension and revocation administrative proceedings. The Coast Guard concurred with each recommendation.

(OIG-10-107, August 2010, ISP)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-107\\_Aug10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-107_Aug10.pdf)

#### ***Allegations of Misconduct Within the Coast Guard Administrative Law Judge Program (Redacted)***

At the request of the Vice-Commandant for the Coast Guard, we initiated a review to determine the merits of a former Coast Guard Administrative Law Judge's allegations of bias within the Coast Guard's ALJ program. We initiated a review to determine whether the Chief ALJ directed subordinate ALJs to rule in favor of the Coast Guard and discussed desired outcomes in specific cases with other ALJs and other employees.

We were not able to substantiate the former ALJ's allegations. We did not determine that the Chief ALJ and others made the alleged remarks, or that the remarks, if made, meant that the Chief ALJ and others engaged in misconduct by directing subordinate ALJs to rule in favor of the Coast Guard. There was no evidence supporting the former ALJ's claim that the Chief ALJ held improper conversations with other ALJs about desired outcomes in specific cases or otherwise deprived mariners of due process in administrative proceedings. We did determine that the Chief ALJ instructed the former ALJ to follow regulations because she was not following regulations. The former ALJ's behavior undermined the gravity of the allegations, which

reinforced our conclusions and led us to doubt her claims. We made no recommendations in this report.

(OIG-10-108, August 2010, ISP)

[http://www.dhs.gov/xoig/assets/mgmtrpts/OIG\\_10-108\\_Aug10.pdf](http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_10-108_Aug10.pdf)

## INVESTIGATIONS

### ***Marine Navigation Equipment Supplier Reaches Settlement***

We and the General Services Administration Office of Inspector General (GSA OIG) and the Naval Criminal Investigative Service (NCIS) conducted an investigation into the allegation that a government contracting corporation provided electronic marine navigation equipment in violation of the *Trade Agreements Act* (TAA). The investigation arose from a qui tam lawsuit that alleged the products the contractor supplied to the U.S. government were produced in a country not authorized to produce end products to the United States under the TAA. Our investigation revealed that the bulk of the contractor's unauthorized marine navigation equipment was delivered to the USCG under a \$5.5 million contract. The Department of Justice reached a settlement agreement with the contractor in the amount of \$695,063.

### ***Two USCG Civilian Employees Resign Amid Investigation Into Possible Compromise of U.S. Coast Guard IT Systems***

We entered into a joint investigation with the U.S. Coast Guard Criminal Investigative Service concerning the unauthorized removal, and subsequent reinstallation into a system intended to process classified material, of computer hardware servers from a USCG facility, in violation of various DHS and USCG IT security policies. A USCG civilian supervisor granted permission to a USCG civilian employee to engage in the unauthorized action. Applicable USCG elements worked jointly with us in an effort to detect any degree of systems compromise. The employees were placed on immediate suspension with all accesses and clearances revoked. The two employees resigned from the USCG while under investigation.

## UNITED STATES CUSTOMS AND BORDER PROTECTION

### MANAGEMENT REPORTS

#### ***Controls Over SBInet Program Cost and Schedule Could Be Improved***

Customs and Border Protection needs to improve its control of contractor activities on the Secure Border Initiative (SBI) technology program. Specifically, program officials did not ensure that contractors maintain up-to-date information in the primary management tool designed to provide managers with advance information regarding potential cost overruns and program progress. In addition, SBInet program officials did not ensure that a program event was properly completed before progressing to the next event and did not adequately document their review and acceptance of accomplishments and criteria at program events. Finally, the low number of government personnel to oversee contractor activities increased the SBInet program office's risk that program cost and schedule could not be adequately managed. Consequently, the SBI program office's ability to ensure that both current and future program goals are accomplished is reduced. We made four recommendations to enhance the program office's ability to ensure that costs are contained, schedules are met, and performance requirements are accomplished.

(OIG-10-96, June 2010, OA)

[http://www.dhs.gov/xoig/assets/mgmtrpts/OIG\\_10-96\\_Jun10.pdf](http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_10-96_Jun10.pdf)

#### ***Information Technology Management Letter for the FY 2009 U.S. Customs and Border Protection (CBP) Financial Statement Audit (Redacted)***

We contracted the independent public accounting firm KPMG to perform the audit of CBP Consolidated Financial Statements as of September 30, 2009. As part of this review, KPMG noted certain matters involving internal control and other operational matters with respect to information technology 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 CBP's financial processing environment

and related IT infrastructure. KPMG noted that CBP took corrective action to address many prior years, IT control weaknesses. However, during FY 2009, KPMG 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 considers them to collectively represent a material weakness under standards established by the American Institute of Certified Public Accountants.

(OIG-10-109, August 2010, IT-A)

[http://www.dhs.gov/xoig/assets/mgmtrpts/OIGr\\_10-109\\_Aug10.pdf](http://www.dhs.gov/xoig/assets/mgmtrpts/OIGr_10-109_Aug10.pdf)

#### **Customs and Border Protection's Importer Self-Assessment**

This audit was initiated in response to a congressional request from U.S. Sen. Charles Grassley, Ranking Member, Senate Committee on Finance. Our objective was to determine the efficacy of the Importer Self-Assessment (ISA) program, by which CBP permits participating importers to assess their own compliance with federal trade requirements in exchange for decreased government oversight and other benefits. We concluded that CBP has not fully established key management controls over the ISA program. Specifically, CBP has not clearly defined the ISA program's purpose, established adequate performance measures, issued uniform formal procedures, verified the effectiveness of applicant importers' internal controls prior to acceptance into the program, or exercised effective oversight of participating importers' compliance with program requirements. Consequently, CBP does not have adequate assurance that participating importers are complying with federal trade requirements and, therefore, that government revenues are being protected. We recommended that the CBP Assistant Commissioner for the Office of Interna-

tional Trade develop policies and procedures to strengthen internal controls over ISA program operations, assess and mitigate current risks to importer trade compliance, and improve oversight of participating importers. CBP concurred with our four recommendations.

(OIG-10-113, August 2010, OA)

[http://www.dhs.gov/xoig/assets/mgmtrpts/OIG\\_10-113\\_Aug10.pdf](http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_10-113_Aug10.pdf)

#### **CBP's Handling of Unaccompanied Alien Children**

The *Flores v. Reno Settlement Agreement* governs the treatment of unaccompanied alien children, minors less than 18 years old who arrive in the United States without a parent or legal guardian and are in federal custody. DHS is bound by the agreement, which includes requirements that immigration officials provide (1) food and drinking water, (2) medical assistance in the event of emergencies, (3) toilets and sinks, (4) adequate temperature control and ventilation, (5) adequate supervision to protect minors from others, and (6) separation from unrelated adults whenever possible.

CBP is one of DHS' immigration enforcement agencies that handles unaccompanied children. CBP personnel apprehend, process, and detain unaccompanied alien children intercepted along the borders and at ports of entry for attempting to enter the United States illegally.

Based on site visits to 30 border patrol stations and ports of entry, document reviews, and independent observations, we concluded that CBP complied with the general provisions of the agreement. Although no significant violations were identified, we made eight recommendations that the agency (1) evaluate its food-purchasing and contracting methods to reduce waste; (2) inform detainees that drinking water in hold rooms was safe; (3) determine the medical needs of unaccompanied alien children; (4) document medical care provided; (5) maintain sufficient medical supplies at detention facilities; (6) inspect toilets and sinks to ensure proper operation; (7) verify that all required personnel complete the mandatory annual

refresher training, and (8) consistently document required information pertaining to unaccompanied alien children.

(OIG-10-117, September 2010, ISP)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-117\\_Sep10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-117_Sep10.pdf)

## INVESTIGATIONS

### ***Mexican National Attempted to Bribe a CBP Officer***

We arrested a Mexican national after he offered a bribe to a CBP Officer (CBPO) at a land border port of entry. The Mexican national attempted to enter the United States presenting a passport issued to another as proof of identity and citizenship. When the CBPO denied entry and took the Mexican national into custody, he offered the CBPO a bribe of \$3,000 to release him and allow him entry into the United States. The Mexican national entered a plea agreement with the United States Attorney's Office and was sentenced to time served plus 12 months' supervised release.

### ***CBPO Sentenced for Bribery and Importation of Controlled Substances***

A CBPO was arrested and was subsequently sentenced to 37 months' incarceration for bribery, misuse of a government computer, and aiding the importation of controlled substances. We were advised by a source that the CBPO was interested in earning money through criminal activity. The source met the CBPO several times over a period of months, at which point the CBPO agreed to allow 5 to 10 kilograms of cocaine into the United States for \$10,000 bribe while the CBPO manned the primary vehicle inspection lane at his port of entry. The CBPO was paid for his role in facilitating and allowing the entry of the purported cocaine, then subsequently arrested.

### ***CBPO Sentenced to 30 Months Prison in for Alien Smuggling***

A CBPO pleaded guilty to a two-count indictment for alien smuggling and identity theft. She also agreed to forfeit her vehicle, which was used in furtherance of the crime. The CBPO and her boyfriend were arrested at a U.S.-Mexico port of entry as they attempted to smuggle an undocumented alien into the United States via the

CBPO's personally owned vehicle. Her accomplice and co-conspirator cooperated with us and agreed to testify against the CBPO. He also told us that this was the fourth occasion that she had smuggled aliens into the United States in her vehicle. As part of his plea agreement, he was allowed to plead guilty to alien smuggling (misdemeanor), and aiding and abetting, and as a U.S. legal permanent resident and citizen of another country was given time served and turned over to the custody of the United States Immigration and Customs Enforcement (ICE) for deportation. The CBPO was sentenced to 30 months in prison followed by 3 years' supervised release.

### ***Three DHS Officers Guilty of Airport Narcotic Smuggling***

***(Update: 4/01/09 – 9/30/09 SAR and 10/01/09 – 3/31/10 SAR)***

We conducted an investigation involving two former CBPOs, who pleaded guilty in federal court to knowingly and intentionally importing into the United States a controlled substance—to wit, 1 kilogram or more of a mixture and substance containing heroin. We had previously arrested a civilian who was the primary organizer of the drug-smuggling conspiracy and a former TSA Supervisory Transportation Security Officer. The three DHS employees used their positions at the U.S. international airport where they were assigned to facilitate the smuggling of illegal narcotics. The civilian conspirator was sentenced to 262 months' confinement, the former TSA supervisor to 135 months' confinement, one of the CBPOs to 120 months' confinement, and the final CBPO was recently sentenced to 168 months' incarceration.

### ***CBPO and Three Civilians Plead Guilty to Narcotic and Alien Smuggling***

We participated in a multiagency task force which included ICE and CBP Office of Internal Affairs that resulted in the arrest of a CBPO and three civilian co-conspirators involved in an alien smuggling conspiracy, importation of controlled substances, and bribery of public officials. The four individuals pleaded guilty in federal court to conspiracy to import more than 100 kilograms of marijuana into the United States, conspiracy to

smuggle undocumented aliens, and bribery of a public official. The former CBPO was sentenced to 20 years in federal prison, and her three civilian co-defendants were sentenced to federal prison for sentences ranging from 24 to 63 months' incarceration. Prior to his arrest, an additional co-defendant in this investigation was murdered in Juarez, Mexico, on February 24, 2010.

#### ***Background Investigator Guilty of False Statements***

We conducted an investigation of a DHS contract background investigator who was subsequently sentenced in federal court to 12 months' probation and fined \$500 for false statements relating to his theft of government funds. We were notified that during an agency routine quality control check, it was discovered that the contract background investigator may have been involved in two incidents of "ghost writing" related to background investigations he had conducted on applicants for employment with CBP. Our investigation determined that the contractor indicated in his background security investigations that he was interviewing people associated with the investigation, but in reality he was not conducting the interviews. He was indicted on six counts of false statements to a government agency.

#### ***Former BPA Sentenced to 6 Years Incarceration (Update 10/01/09 - 3/31/10 SAR)***

In 2006, we initiated an investigation concerning allegations that a Border Patrol Agent (BPA) was involved in narcotic smuggling on the southwest border. The BPA facilitated the shipment and transportation of illicit drugs (cocaine and marijuana) by providing protective escorts in exchange for bribe payments, which allowed the illicit drugs to avoid detection by other law enforcement officers. After an extensive investigation, the BPA appeared this summer in federal court for sentencing following a plea agreement with the U.S. Attorney's Office, on charges related to a public official accepting a bribe and the attempt to aid and abet the possession with intent to distribute 5 kilograms of cocaine. The BPA was sentenced to 72 months for each count with sentences to run concurrently, followed by 3 years' supervised release. As part of his plea agreement,

the BPA agreed to cooperate with us in a full debriefing interview.

#### ***CBP Employee Sentenced to 6 Years for Possession of Child Pornography***

We participated in a child pornography investigation resulting in the arrest of a CBP supervisory chemist. We, along with ICE OPR and the FBI, executed a federal (FBI) search warrant at the residence of the CBP chemist as part of an ongoing Internet child pornography materials investigation. Prior to the search, the CBP employee provided a full confession of his involvement with the acquisition and sharing of illegal child pornographic material via his personal residential computer(s). The employee pleaded guilty to one felony count of receipt of child pornography, was sentenced to 72 months' incarceration followed by 60 months' probation, and has resigned from CBP.

#### ***BPA Pleads Guilty to Accepting a Bribe***

We participated in an FBI task force's arrest of a BPA who was charged with selling DHS Border Patrol sensor maps and assisting with the smuggling of narcotics along the U.S.-Mexican border. The BPA pleaded guilty in federal court to one count of a public official accepting a bribe. Sentencing is scheduled for November 15, 2010.

#### ***CBPO Pleads Guilty to Possession of Child Pornography***

A CBPO pleaded guilty in federal court to possession of child pornography. We received an allegation that the CBPO was using the Internet to engage in sexually explicit conversations with juveniles and view child pornographic images, using his personal laptop computer. The CBPO was the subject of an earlier local police report alleging that a former girlfriend found pornographic images of underage individuals on his laptop computer. We interviewed the CBPO and obtained a confession. He admitted to being addicted to pornography and to visiting child pornographic websites on a regular basis. He consented to a search of his laptop computer, which was turned over to the United States Secret Service for forensic testing. Forensic testing resulted in the recovery of at least 40 images, which were previously identified as sexually explicit child pornography by the National Association for Missing and Exploited Children.

## UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT

### MANAGEMENT REPORTS

#### *Information Technology Management Letter for the FY 2009 Immigration Customs Enforcement Financial Integrated Audit*

We contracted the independent public accounting firm KPMG to perform the audit of Immigration and Customs Enforcement (ICE) consolidated balance sheet in support of DHS' financial statement audit as of September 30, 2009. As part of this review, KPMG noted certain matters involving internal control and other operational matters with respect to information technology 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 ICE's financial processing environment and related IT infrastructure. KPMG noted that ICE took corrective action to address many prior years' IT control weaknesses. However, during FY 2009, KPMG continued to find IT general control weaknesses at ICE. The most significant weaknesses from a financial statement audit perspective related to controls over the FFMS and the weaknesses over 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 considers them to collectively represent a material weakness under standards established by the American Institute of Certified Public Accountants.

(OIG-10-87, May 2010, IT-A)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-87\\_May10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-87_May10.pdf)

#### *Immigration and Customs Enforcement Information Technology Management Progresses But Challenges Remain*

ICE's Office of the Chief Information Officer (OCIO) provides IT services and solutions in support of the ICE mission. We reviewed ICE's IT management functions in order to determine whether the component's IT management approach adequately addresses strategic planning, implementation, and management of technology to support its goals.

ICE has improved its strategic planning; however, it has not yet finalized its IT strategic plan. Further, although the OCIO has oversight of IT spending, its budget planning process did not capture all the component's IT needs. Finally, the OCIO is challenged to deliver effective IT services and support owing to conflicting priorities and staffing shortages. We recommend that the ICE Assistant Secretary (1) finalize an agency-wide IT Strategic Plan to establish and communicate IT strategic goals and objectives to stakeholders, (2) establish an agency-wide IT budget process to include all ICE component office technology initiatives and requirements, (3) develop an OCIO staffing plan that includes specific actions and milestones for recruiting and retaining fulltime employees, and (4) establish a formal process to facilitate IT policy development, approval, and dissemination.

(OIG-10-90, May 2010, IT-A)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-90\\_May10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-90_May10.pdf)

#### *Immigration and Customs Enforcement Privacy Stewardship*

ICE is the largest DHS investigative agency. ICE is responsible for enforcing immigration laws and investigating people, money, and materials that support terrorist and criminal activities. Almost 18,000 employees in more than 400 offices around the world interact daily with the public or collect, use, and disseminate personally identifiable information (PII) about the public. Our audit objectives were to determine whether ICE's plans and activities instill a culture of privacy and whether ICE complies with federal privacy laws and regulations.

ICE has made progress instilling a culture of privacy. Specifically, it demonstrated an organizational commitment to privacy compliance by appointing a privacy officer and establishing the ICE Privacy Office. The Privacy Office provides guidance to program and system managers who collect personally identifiable information on meeting requirements for notice, incident reporting, and privacy impact assessments. In addition, the Privacy Office has established processes for initial and annual privacy training and for addressing access, complaints, and redress for individuals.

ICE can strengthen its privacy stewardship by developing and implementing job-related privacy training and oversight to safeguard PII in program operations, establishing penalties for violations that correspond with DHS privacy rules of conduct, and establishing a standardized process of engagement and role for the ICE Privacy Office in the review and approval of information-sharing access agreements that involve PII.

(OIG-10-100, July 2010, IT-A)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-100\\_Jul10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-100_Jul10.pdf)

#### ***Age Determination Practices for Unaccompanied Alien Children – Update***

This is an update to our report, *Age Determination Practices for Unaccompanied Alien Children* (OIG-10-12), requested by the House Appropriations Committee and House Report 111-157. Our objective was to provide an update to the Congressional Appropriations Committees on actions ICE has taken to address recommendations made in our formerly issued OIG-10-12 review. While ICE uses radiographic exams to help determine individuals' ages in some cases, it recognizes the limits of radiographs and strives to obtain additional information when making age determinations. ICE does not, however, track age determination data, including the number of radiographic exams that are used for age determinations or the number of misplacements of detained juveniles or adults. It also needs to release updated guidance on making age determinations and selecting professionals to provide age estimations based on radiographs. In our initial report, we recommended that ICE

enhance its ability to track data related to age determination, update field guidance on making age determinations, and identify "best-qualified" practitioners to conduct age estimations when practical. ICE expects to complete corrective action for each of these recommendations by December 2010.

(OIG-10-122, September 2010, ISP)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-122\\_Sep10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-122_Sep10.pdf)

#### ***The Performance of 287(g) Agreements Report Update***

This report addresses the performance of 287(g) agreements between ICE and law enforcement agencies, and progress made towards implementing recommendations from our prior report, OIG-10-63, *The Performance of 287(g) Agreements*, issued in March 2010. We also address the use of 287(g) funds, and challenges in conducting compliance reviews of 287(g) agreements, and performance measures used to determine the success of the 287(g) program in achieving its goals. Our objective was to: provide an update to the congressional appropriations committees on action ICE has taken to address our recommendations for the 287(g) program in FY 2010. We determined that ICE needs to continue efforts to implement our prior recommendations and identified challenges that may reduce the effectiveness of a review process intended as a resource for ensuring compliance with 287(g) program requirements. We are making 16 recommendations.

(OIG-10-124, September 2010, ISP)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-124\\_Sep10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-124_Sep10.pdf)

## **INVESTIGATIONS**

### ***ICE Special Agent Pleads Guilty in Bribery Investigation***

A ICE Special Agent was arrested following a 3-year undercover operation conducted by us and ICE OPR, during which the agent received kickbacks from informants and disclosed information to criminal investigative subjects to help them avoid capture by law enforcement. He additionally took money to help smuggle illegal aliens into the country. The agent, who subsequently pleaded guilty to charges of receiving a gratuity by a public

official, faces a maximum sentence of 2 years' imprisonment and a possible fine of \$250,000. The agent has been terminated by ICE.

***ICE Employee Sentenced in Document Fraud Investigation***

***(Update 10/01/09 – 3/31/10 SAR)***

We and the FBI conducted an investigation that resulted in a former Deportation Officer (DO) ICE, Detention and Removal Operations, pleading guilty to obstruction of justice and document fraud and being sentenced to 3 months' confinement, 2 years' supervision, and fined \$4,000. The obstruction count involved his participation in the destruction of master immigration Alien files of deportable aliens with the intent to prevent their deportation. The second count involved his fraudulent issuance of an Alien Documentation Identification and Telecommunication (A.D.I.T.) stamp conveying temporary legal resident status to an alien who was eligible for deportation. As a deportation officer, the subject was responsible for supervising aliens who had been deported but were not in immigration custody. Our investigation determined that the DO accepted bribes from a deportable foreign national to destroy his and his cousin's Alien files, fraudulently placed A.D.I.T. stamps in passports of other deportable aliens, and arranged for the unauthorized release of an alien in ICE custody.

***ICE Agent Pleads Guilty in Narcotics Investigation***

We assisted ICE Office of Investigations (OI) in an investigation of a ICE Detention and Removal Operations Agent who pleaded guilty to a one-count indictment charging that from June 2009 through on or about September 11, 2009, he knowingly and intentionally conspired and agreed with others to distribute and to possess 5 kilograms or more of cocaine. Following an undercover operation, the employee, along with two civilian co-conspirators, were arrested by ICE OI. The agent is no longer employed by ICE.

***ICE Contracting Officer Guilty of Conflict of Interest***

A Mission Support Specialist and Contracting Officer employed by ICE, Detention and Removal

Operations (DRO), entered a guilty plea to one count of felony conflict of interest. The contracting officer was responsible for authorizing the ICE DRO Field Office to enter into contracts for goods and services. Our investigation determined that he steered contracts to companies that he and his wife owned. The employee, who has been suspended from ICE, has agreed to forfeit cash and property valued at \$200,000, and he will be sentenced in federal court in October 2010.

***ICE Employee Sentenced to 48 Months for Firearm and Ammunition Violations***

We and local police investigated a former Immigration and Enforcement Agent (IEA) ICE, DRO who pleaded guilty to one count of unlawful possession of a firearm and one count of possession of stolen ammunition. He was sentenced in federal court to 48 months' imprisonment. Our joint investigation revealed that the former ICE employee was a convicted felon and was in possession of several firearms and items bearing DHS and ICE markings, including a portable radio, ammunition, fraudulent credentials, and replica badges. The former ICE employee admitted to willfully and illegally possessing firearms, failed to return his ICE-issued radio, and took for his personal benefit one case of .40 caliber ammunition from the ICE DRO office. Also, the former employee illegally manufactured, displayed, and carried on his person photocopies of his official ICE DRO credentials, along with a replica of his official ICE DRO badge.

***ICE Agent Guilty of Importing Illegal Steroids***

We and the U.S. Food and Drug Administration, Office of Criminal Investigation, conducted an investigation of a Special Agent, ICE, OI, who pleaded guilty in federal court to importing steroids. This investigation arose out of a complaint alleging that the agent imported steroids and human growth hormones into the United States. Our investigation determined that he utilized a fictitious address, a false telephone number, and a wire transfer to facilitate his purchase. The agent has resigned from ICE, and his sentencing is scheduled for later this year.



### ***Contract Correctional Officer Sentenced for Sexual Abuse of Detainee***

We investigated an allegation against a contract Correctional Officer (CO) involving sexual contact with a federal immigration detainee. We interviewed the CO at the detention facility where he provided a sworn written statement admitting that sexual contact had occurred between himself and a federal detainee, who was a Mexican citizen. The CO subsequently pleaded guilty to sexual abuse of a ward of the government and was sentenced to 10 months' imprisonment, 24 months of supervised release, \$3,000 fine, and a \$100 special assessment fee. Upon notification of the sentencing of the CO, the Mexican consul, New Orleans, LA, said that she would notify the victim and expressed sincere gratitude to the United States and the justice system for the combined efforts in the successful prosecution of the CO.

### ***Vigilante ICE Officer Sentenced to 4 Years for Assault***

We conducted a joint investigation with local police involving allegations of felonious assault, felony firearms violation, and unlawful imprisonment against a Supervisory Deportation Officer, Immigration and Customs Enforcement, Enforcement and Removal Office. The joint investigation resulted in the officer's conviction in state court and subsequent sentencing to 4 years' incarceration. The Supervisory Detention Officer, in an attempt to solve a burglary, forced a citizen into his government-owned vehicle (GOV) at gunpoint. Once in his GOV, the officer drove the victim to an abandoned house, where he began to beat the victim with his duty weapon. At some point the officer placed his duty weapon in the victim's mouth to threaten him. The victim was able to escape after the officer fired a round from his duty weapon. Two days later, the officer approached a second citizen, pushed him to the ground, and then threatened the victim with his duty weapon as he questioned him about the same burglary.

### ***ICE Agent Imposter Pleads Guilty in State and Federal Court for Operating a "Large-Scale Cash for Immigration Benefits" Fraud Scheme***

We conducted a joint investigation with ICE and local police concerning a group of individ-

uals posing as ICE officials who were allegedly requesting large sums of money in exchange for purportedly being able to provide authentic immigration benefit documents to illegal immigrants from across the United States. The victims of the group believed the group to be legitimately assisting many aliens whose family members needed immigration assistance, and as such paid them with an understanding that they and/or their family members would attain official U.S. citizenship status, as promised by the group. The ringleader was dressed in a DHS/ICE uniform, claiming to be working for ICE, and has pleaded guilty in state court to five counts of felony theft, one count of participation in a felony theft scheme, and one count of conspiracy to commit theft over \$100,000. A sentencing date of November 1, 2010, is scheduled in state court. Additionally, the ringleader pleaded guilty in federal court to one count of transportation of money obtained by fraud, one count of conspiracy, and one count of felon in possession of ammunition. A sentencing date in federal court is pending. Judicial action continues against the co-conspirators in the investigation.

## **MULTIPLE COMPONENTS**

### **MANAGEMENT REPORTS**

#### ***DHS' Counterintelligence Activities***

We assessed DHS's counterintelligence activities as part of our FY 2009 Annual Performance Plan. Specifically, we focused on the program's history, evolution, activities, and coordination and collaboration efforts. DHS is one of the largest and most visible federal departments. Throughout DHS, designated personnel have access to classified information and systems. Protecting the department involves safeguarding personnel, information, operations, programs, and technologies from intelligence threats. To counter these threats, the department has developed capabilities to detect and neutralize intelligence vulnerabilities.

The DHS Counterintelligence Program conducts the department's counterintelligence mission activities at the direction of, and under the authority of the Secretary. The primary mission

of the DHS Counterintelligence Program is to prevent adversaries from penetrating the department to exploit sensitive information, operations, programs, personnel, and resources. In addition, the United States Coast Guard provides Coast Guard specific counterintelligence support to the department. Their primary mission is to preserve operational integrity by shielding operations, personnel, systems, facilities, and information from intelligence threats. Although the United States Coast Guard has been successful in developing its counterintelligence program, the DHS Counterintelligence Program has experienced some organizational challenges. We made multiple recommendations to help the department enhance its coordination of counterintelligence activities, define roles and responsibilities, and to improve its oversight.

(OIG-10-97, June 2010, ISP)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-97\\_Jun10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-97_Jun10.pdf)

***Review of the Department of Homeland Security's Master List of Recovery Act Contracts and Grants***

At the request of the Recovery Accountability and Transparency Board, we reviewed the DHS Master List of *Recovery Act* Contracts and Grants to determine whether the contract and grant award amounts in the Master List were accurate. With minor exceptions, the DHS Master List of *Recovery Act* Contracts and Grants was accurate for the period ending March 31, 2010. DHS will have to periodically update the Master List as its components obligate additional *Recovery Act* funds. In doing so, DHS agreed with our recommendation to implement controls to ensure that its updates are accurate.

(OIG-10-102, July 2010, OA)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-102\\_Jul10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-102_Jul10.pdf)

***Audit of Department of Homeland Security's Handling of Conference Fees for the Process Control Systems Forum***

The Science and Technology Directorate awarded a contract to a private contractor on October 13, 2004, to create and manage a Process Control Systems Forum. On June 27, 2006, a modification to the contract transferred forum responsibility to the National Protection and Programs Directorate; however, forum funding continued to be provided from Science and Technology's appropriation. In 2008, concerns were raised that forum conference fees had been inappropriately collected. The Office of the Chief Financial Officer referred the matter to us for review on November 25, 2008. We performed our audit to determine whether the receipt of conference registration fees violated the Miscellaneous Receipts Statute (31 U.S.C. 3302) or the *Anti-deficiency Act* (31 U.S.C. 1351 and 31 U.S.C. 1517 (a)). Our review determined that DHS violated the Miscellaneous Receipts Statute by improperly augmenting its appropriations with the conference fees collected in FYs 2005 to 2007 and not remitting those fees to the U.S. Treasury general fund as required. However, DHS did not violate the *Anti-deficiency Act* because appropriated funds available from the years in question are sufficient to cover remittance of the conference fees to the U.S. Treasury Account. We recommended that DHS remit to the U.S. Treasury Fund the \$211,445 in conference registration fees for the Process Control Systems Forum in FYs 2005 through 2007. Both directorates concurred with the recommendation.

(OIG-10-104, July 2010, OA)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_10-104\\_Jul10.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-104_Jul10.pdf)

***Evaluation of DHS' Security Program and Practices for Its Intelligence Systems for Fiscal Year 2010***

We reviewed DHS' enterprise-wide security program and practices for its Top Secret/Sensitive Compartmented Information intelligence systems. Pursuant to the *Federal Information Security Management Act* (FISMA) 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 continues to maintain an effective enterprise-wide information security management program for its intelligence systems. Overall, DHS has developed information security procedures and implemented effective security controls on its intelligence systems. Nonetheless, management oversight and operational issues remain regarding the effectiveness of the program. Concerns with system Certification and Accreditation documentation and the implementation of a formal information system security training and awareness program for intelligence personnel still exist. Further, because the Intelligence and Analysis Office is now responsible for the U.S. Coast Guard intelligence systems reporting, the office should continue to provide management oversight to ensure that the U.S. Coast Guard maintains an effective information technology security program and complies with FISMA and DHS requirements. Our report to the Inspector General Office of the Director of National Intelligence did not contain any recommendations.

(OIG-10-112, August 2010, IT-A)

[http://www.dhs.gov/xoig/assets/mgmtrpts/OIG\\_10-112\\_Aug10.pdf](http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_10-112_Aug10.pdf)

# OTHER OFFICE OF INSPECTOR GENERAL ACTIVITIES



## OVERSIGHT OF NONDEPARTMENTAL AUDITS

During this period, we 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.

## 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 159 reports containing 479 recommendations that have been unresolved for more than 6 months. Management decisions have not been made for significant reports, as follows:

91	FEMA-related financial assistance disaster audits
68	Program management reports
<b>159</b>	<b>Total</b>

## OVERSIGHT OF DEPARTMENTAL AUDITS

### *An IG’s Guide for Assessing Federal Response Capabilities*

The National Response Framework (NRF) emphasizes the importance of engaged partnerships to enhance our Nation’s preparedness to respond to domestic threats and disasters. The federal government maintains a wide array of capabilities and resources that can be made available in response to a disaster. No fewer than 12 federal departments and agencies have key Emergency Support Function roles and responsibilities outlined in the NRF. When an incident occurs that exceeds local and state resources, the federal government uses the NRF to engage all necessary department and agency capabilities, organize the response, and ensure coordination with response partners.

The Emergency Management Working Group, a subgroup of the Council of Inspectors General on Integrity and Efficiency (CIGIE), developed “An IG’s Guide for Assessing Federal Response Capabilities” as a resource available to the Inspector General community to assess a department’s or agency’s capabilities based on their respective Emergency Support Function roles and responsibilities enumerated in the National Response Framework. The guide is a collaborative effort by staff from numerous Inspector General offices, and has already been used by several Inspector General offices, including DHS, the Department of Defense, the Department of Energy, the Department of the Interior, and the Department of Agriculture.

<http://www.ignet.gov/randp/igguidefederalresponse0810.pdf>

# LEGISLATIVE AND REGULATORY REVIEW



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 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 over 100 legislative and regulatory proposals, draft DHS policy directives, and other items. Two of these items are highlighted below.

***H.R. 5815, Inspector General Authority Improvement Act of 2010, With Cuellar Amendment***

This bill, if enacted, would provide Inspectors General with testimonial subpoena authority. We strongly favor obtaining such authority, but are concerned with the provision granting the Department of Justice (DOJ) veto power over testimonial subpoenas issued for investigations

of alleged violations of criminal law or the *False Claims Act*. Although this would be an improvement on the current law, the Department of Defense (DOD) IG recently obtained testimonial subpoena authority that does not provide for DOJ veto power in any case. DOD is simply required to notify DOJ 7 days in advance of issuing subpoenas for testimony. Thus, we recommended legislative revisions to ensure that other IGs have the same testimonial subpoena authority that is provided to DOD under section 8(i) of the *Inspector General Act*.

***United States Office of Personnel Management (OPM) Final Rule Titled “Recruitment, Selection, and Placement (General)”***

We were asked to review the final rule whereby OPM is revising the regulations on federal vacancy announcements, reemployment priority list requirements, positions restricted to preference eligibles, the restriction on moving an employee immediately after a competitive appointment, the Career Transition Assistance Plan, and the Interagency Career Transition Assistance Plan. This final rule clarifies the regulations, incorporates longstanding OPM policies, revises placement assistance programs for consistency and effectiveness, removes references to two expired interagency placement assistance programs, and reorganizes information for ease of reading. We had no objections to this rule.

# CONGRESSIONAL TESTIMONY AND BRIEFINGS





The Inspector General and senior executives testified before congressional committees eight times. Testimony prepared for these hearings may be accessed on our website at [www.dhs.gov/voig](http://www.dhs.gov/voig).

We testified on the following issues:

- April 21, 2010 - Senate Commerce, Science and Transportation Committee, on “Securing the Nation’s Rail and Other Surface Transportation Networks.”
- May 12, 2010 - Senate Committee on Homeland Security and Governmental Affairs’ Ad Hoc Subcommittee on Disaster Recovery, on “*Stafford Act Reform: Sharper Tools for a Smarter Recovery.*”
- June 16, 2010 - House Homeland Security Committee, on “Cybersecurity: DHS’ Role, Federal Efforts, and National Policy.”
- June 29, 2010 - House Committee on Homeland Security’s Subcommittee on Emergency Communications, Preparedness and Response, on “The Future of FEMA’s Grant Programs Directorate.”
- July 28, 2010 - House Committee on Homeland Security’s Subcommittee on Transportation Security and Infrastructure Protection, on “Lost in the Shuffle: Examining TSA’s Management of Surface Transportation Security Inspectors.”
- September 22, 2010 - House Homeland Security Committee, on “DHS Planning and Response: Preliminary Lessons From Deepwater Horizon.”
- September 22, 2010 - House Transportation and Infrastructure’s Subcommittee on Economic Development, Public Buildings and Emergency Management on “Five Years After Katrina: Where We Are and What We Have Learned for Future Disasters.”
- September 29, 2010 - House Committee on Homeland Security’s Subcommittee on Emergency Communications, Preparedness and Response, on “Emergency Logistics Management: Transforming the Delivery of Disaster Relief for the 21st Century.”

We briefed congressional members and their staff at a steady pace throughout the reporting period. Our office conducted more than 30 briefings for congressional staff on the results of our work, including reviews of (1) *DHS Use of Suspension and Debarment Actions for Poorly Performing Contractors* (OIG-10-50), (2) *TSA Acquisition of Support Services Contracts* (OIG-10-72), (3) *Management Advisory Report: Permanent Housing Construction on American Samoa* (OIG-10-74), and (4) *Evaluation of Passenger Screening Technology* (OIG-10-75). We attended meetings to discuss other congressional concerns, including our investigative work, TSA’s surface inspectors program, cybersecurity, and science and technology.

# APPENDICES



## Appendix 1

# Audit Reports With Questioned Costs

Report Category	Number	Questioned Costs	Unsupported Costs
<b>A.</b> Reports pending management decision at the start of the reporting period	150	\$191,001,193	\$33,119,236
Plus prior period adjustments (a)	2	\$21,582,893	\$1,503,836
<b>B.</b> Reports issued/processed during the reporting period with questioned costs	23	\$77,597,951	\$24,976,746
<b>TOTAL REPORTS (A+B)</b>	<b>175</b>	<b>\$290,182,037</b>	<b>\$59,599,818</b>
<b>C.</b> Reports for which a management decision was made during the reporting period (b)	10	\$17,038,381	\$6,804,267
(1) Disallowed costs	9	\$16,087,386	\$6,349,953
(2) Accepted costs	5	\$950,995	\$454,314
<b>D.</b> Reports put into appeal status during period	0	\$0	\$0
<b>E.</b> Reports pending a management decision at the end of the reporting period	165	\$273,143,656	\$52,795,551
<b>F.</b> Reports for which no management decision was made within 6 months of issuance	142	\$195,545,705	\$27,818,805

### 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	25	\$24,081,803
B. Reports issued during the reporting period	10	\$53,241,230
<b>Total Reports (A+B)</b>	<b>35</b>	<b>\$77,323,033</b>
C. Reports for which a management decision was made during the reporting period	5	\$4,233,779
(1) Value of recommendations agreed to by management for deobligation	5	\$4,233,779
(2) Value of recommendations not agreed to by management	0	\$0
D. Reports put into the appeal status during the reporting period	0	\$0
E. Reports pending a management decision at the end of the reporting period.	30	\$73,089,254
F. Reports for which no management decision was made within 6 months of issuance	20	\$19,848,024

#### Notes and Explanations:

**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**

<b>MANAGEMENT DECISION IS PENDING</b>	
<b>3/31/10</b>	
Reports open and unresolved more than 6 months	202
Recommendations open and unresolved more than 6 months	675
<b>9/30/10</b>	
Reports open and unresolved more than 6 months	159
Recommendations open and unresolved more than 6 months	479
<b>CURRENT INVENTORY</b>	
Open reports at the beginning of the period	359
Reports issued this period	77
Reports closed this period	50
Open reports at the end of the period	386
<b>ACTIVE RECOMMENDATIONS</b>	
Open recommendations at the beginning of the period	1,785
Recommendations issued this period	260
Recommendations closed this period	414
Open recommendations at the end of the period	1,631

## Appendix 3

# Management Reports Issued

Report Number	Date Issued	Report Title	Questioned Costs	Unsupported Costs	Funds Put to Better Use
1. OIG-10-77	4/10	Information Technology Management Letter for the United States Coast Guard Component of the FY 2009 DHS Integrated Audit	\$0	\$0	\$0
2. OIG-10-78	4/10	Independent Auditors' Report on Transportation Security Administration's Consolidated Balance Sheet as of September 30, 2009	\$0	\$0	\$0
3. OIG-10-79	4/10	Management Letter for the Transportation Security Administration's Consolidated Balance Sheet as of September 30, 2009	\$0	\$0	\$0
4. OIG-10-80	4/10	The Responsibilities of the Office of Counter narcotics Enforcement	\$0	\$0	\$0
5. OIG-10-81	4/10	NPSC Preparedness for Large-Scale Disasters	\$0	\$0	\$0
6. OIG-10-82	4/10	Information Technology Management Letter for the FY 2009 Transportation Security Administration Financial Integrated Audit	\$0	\$0	\$0
7. OIG-10-83	4/10	Information Technology Management Letter for the FY 2009 Federal Law Enforcement Training Center Financial Statement Audit	\$0	\$0	\$0
8. OIG-10-84	4/10	Coast Guard's Blueprint for Acquisition Reform Needs Improved Oversight	\$0	\$0	\$0
9. OIG-10-85	5/10	The Coast Guard's Boat Crew Communications System Is Unreliable	\$0	\$0	\$0
10. OIG-10-86	5/10	Stronger Security Controls Needed on Active Directory Systems	\$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-10-87	5/10	Information Technology Management Letter for the FY 2009 Immigration Customs Enforcement Financial Integrated Audit	\$0	\$0	\$0
12. OIG-10-88	5/10	Special Report: Summary of Significant Investigations October 1, 2008, to September 30, 2009	\$0	\$0	\$0
13. OIG-10-89	5/10	The Coast Guard's Maritime Safety and Security Team Program	\$0	\$0	\$0
14. OIG-10-90	5/10	Immigration and Customs Enforcement Information Technology Management Progresses, but Challenges Remain	\$0	\$0	\$0
15. OIG-10-91	5/10	Improving FEMA's Disaster Purchase Card Program	\$0	\$0	\$0
16. OIG-10-92	5/10	Information Technology Management Letter for the Federal Emergency Management Agency Component of the FY 2009 DHS Integrated Audit	\$0	\$0	\$0
17. OIG-10-93	6/10	Information Technology Management Letter for the FY 2009 U.S. Citizenship and Immigration Services Financial Statement Audit	\$0	\$0	\$0
18. OIG-10-94	6/10	U.S. Computer Emergency Readiness Team Makes Progress in Securing Cyberspace, but Challenges Remain	\$0	\$0	\$0
19. OIG-10-95	6/10	DHS Needs to Address Challenges to Its Financial Systems Consolidation Initiative	\$0	\$0	\$0
20. OIG-10-96	6/10	Controls Over SBlNet Program Cost and Schedule Could Be Improved	\$0	\$0	\$0
21. OIG-10-97	6/10	DHS' Counterintelligence Activities (Summary)	\$0	\$0	\$0

## Appendix 3

### Management Reports Issued (continued)

Report Number	Date Issued	Report Title	Questioned Costs	Unsupported Costs	Funds Put to Better Use
22. OIG-10-98	6/10	FEMA's Disaster Assistance Improvement Plan	\$0	\$0	\$0
23. OIG-10-99	7/10	Management Oversight and Component Participation Are Necessary to Complete DHS' Human Resource Systems Consolidation Effort	\$0	\$0	\$0
24. OIG-10-100	7/10	Immigration and Customs Enforcement Privacy Stewardship	\$0	\$0	\$0
25. OIG-10-101	7/10	FEMA's Logistics Management Process for Responding to Catastrophic Disasters	\$0	\$0	\$0
26. OIG-10-102	7/10	Review of the Department of Homeland Security's Master List of Recovery Act Contracts and Grants	\$0	\$0	\$0
27. OIG-10-103	7/10	Special Review of the Science and Technology Directorate's Contracts With a Small Business (Summary)	\$0	\$0	\$0
28. OIG-10-104	7/10	Audit of the Department of Homeland Security's Handling of Conference Fees for the Process Control Systems Forum	\$0	\$0	\$0
29. OIG-10-105	8/10	Funding Plan for the United States Coast Guard Museum	\$0	\$0	\$0
30. OIG-10-106	8/10	Annual Review of the United States Coast Guard's Mission Performance (FY 2009)	\$0	\$0	\$0
31. OIG-10-107	8/10	Recommendations to Improve the Coast Guard's System for Adjudicating Suspension and Revocation Matters	\$0	\$0	\$0



## Appendix 3

### Management Reports Issued (continued)

Report Number	Date Issued	Report Title	Questioned Costs	Unsupported Costs	Funds Put to Better Use
32. OIG-10-108	8/10	Allegations of Misconduct Within the Coast Guard Administrative Law Judge Program (Redacted)	\$0	\$0	\$0
33. OIG-10-109	8/10	Information Technology Management Letter for the FY 2009 U.S. Customs and Border Protection Financial Statement Audit (Redacted)	\$0	\$0	\$0
34. OIG-10-110	8/10	Information Technology Management Letter for the FY 2009 DHS Integrated Audit (Redacted)	\$0	\$0	\$0
35. OIG-10-111	8/10	DHS Needs to Improve the Security Posture of Its Cybersecurity Program Systems	\$0	\$0	\$0
36. OIG-10-112	8/10	Evaluation of DHS' Security Program and Practices for Its Intelligence Systems for Fiscal Year 2010 (Unclassified Summary)	\$0	\$0	\$0
37. OIG-10-113	8/10	Customs and Border Protection's Importer Self-Assessment Program	\$0	\$0	\$0
38. OIG-10-114	8/10	Federal Emergency Management Agency Mount Weather Emergency Operations Center Tenant Satisfaction Survey (Unclassified Summary)	\$0	\$0	\$0
39. OIG-10-115	9/10	FEMA's Management of Disaster Assistance Employee Deployment and Payroll Processes	\$0	\$0	\$0
40. OIG-10-116	9/10	The State of Maryland's Management of State Homeland Security Program and Urban Areas Security Initiative Grants Awarded During Fiscal Years 2005 Through 2007	\$54,313	\$54,313	\$0

## Appendix 3

### Management Reports Issued (continued)

Report Number	Date Issued	Report Title	Questioned Costs	Unsupported Costs	Funds Put to Better Use
41. OIG-10-117	9/10	CBP's Handling of Unaccompanied Alien Children	\$0	\$0	\$0
42. OIG-10-118	9/10	Efforts to Detect and Deter Fraud Committed by Immigration Services Officers	\$0	\$0	\$0
43. OIG-10-119	9/10	Evaluation of Screening of Air Cargo Transported on Passenger Aircraft (Unclassified Summary)	\$0	\$0	\$0
44. OIG-10-120	9/10	Management of DHS' Data Center Consolidation Initiative Needs Improvement	\$0	\$0	\$0
45. OIG-10-121	9/10	FEMA's Implementation of Recommendations from Top Officials 4	\$0	\$0	\$0
46. OIG-10-122	9/10	Age Determination Practices for Unaccompanied Alien Children – Update	\$0	\$0	\$0
47. OIG 10-123	9/10	FEMA's Preparedness for the Next Catastrophic Disaster – An Update	\$0	\$0	\$0
48. OIG-10-124	9/10	The Performance of 287(g) Agreements Report Update	\$0	\$0	\$0
		<b>Total, Appendix 3</b>	<b>\$54,313</b>	<b>\$54,313</b>	<b>\$0</b>

### Notes and Explanations:

#### Report Number Acronym:

OIG – Management report

## Appendix 4

### Financial Assistance Audit Reports Issued

Report Number	Date Issued	Report Title	Questioned Costs	Unsupported Costs	Funds Put to Better Use
1. DA-10-10	5/10	City of Buffalo, New York	\$3,263,967	\$727,138	\$0
2. DA-10-11	6/10	City of Pass Christian, Mississippi	\$202,583	\$202,583	\$577,710
3. DA-10-12	6/10	City of Hialeah, Florida	\$2,511,948	\$115,242	\$0
4. DA-10-13	7/10	Virgin Islands Water and Power Authority	\$0	\$0	\$0
5. DA-10-14	7/10	Hancock County School District, Mississippi	\$669,683	\$0	\$35,119
6. DA-10-15	7/10	South Mississippi Electric Power Association	\$1,542,153	\$0	\$0
7. DA-10-16	8/10	Mississippi Coast Coliseum Commission	\$518,658	\$0	\$1,620,026
8. DA-10-17	8/10	City of Greenville, South Carolina	\$74,080	\$0	\$0
9. DA-10-18	9/10	Florida Department of Military Affairs	\$1,163,464	\$0	\$0
10. DA-10-19	9/10	City of Fort Lauderdale, Florida	\$15,047,693	\$1,000,083	\$0
11. DD-10-07	3/10	City of North Royalton, Ohio	\$0	\$0	\$0
12. DD-10-08	3/10	Orleans Parish Criminal Sheriff's Office	\$2,472,053	\$0	\$0
13. DD-10-09	4/10	City of Bucyrus, Ohio	\$358,860	\$13,563	\$0
14. DD-10-10	6/10	Nebraska Public Power District, Columbus, Nebraska	\$1,671,599	\$0	\$0
15. DD-10-11	6/10	Management Issues Identified During Hazard Mitigation Grant Audits in the State of Ohio	\$0	\$0	\$0
16. DD-10-12	7/10	Orleans Levee District	\$295,062	\$0	\$0

## Appendix 4

### Financial Assistance Audit Reports Issued (continued)

Report Number	Date Issued	Report Title	Questioned Costs	Unsupported Costs	Funds Put to Better Use
17. DD-10-13	7/10	Greene County, Missouri	\$0	\$0	\$0
18. DD-10-14	7/10	Recovery School District – Abramson High School	\$16,892,149	\$0	\$19,602,818
19. DD-10-15	7/10	Louisiana State University Health Sciences Center	\$0	\$0	\$3,044,234
20. DD-10-16	8/10	Lamar University, Beaumont, Texas	\$25,557,891	\$22,832,786	\$1,377,271
21. DD-10-17	9/10	Louisiana Department of Health and Hospitals	\$0	\$0	\$22,569,311
22. DD-10-18	9/10	Roman Catholic Church of the Archdiocese of New Orleans Contracting and Emergency Protective Measures	\$520,952	\$0	\$0
23. DD-10-19	9/10	Xavier University of Louisiana, Contracting	\$0	\$0	\$0
24. DS-10-06	3/10	County of Mendocino, California	\$21,312	\$0	\$0
25. DS-10-07	4/10	County of Los Angeles, California	\$2,048,890	\$0	\$203,909
26. DS-10-08	6/10	FEMA's Practices for Evaluating Insurance Coverage for Disaster Damage and Determining Project Eligibility and Costs	\$1,313,363	\$0	\$3,920,869
27. DS-10-09	7/10	City of Napa, California	\$492,059	\$0	\$289,963
28. DS-10-10	9/10	City of Glendale, California	\$217,565	\$31,038	\$0
29. DS-10-11	9/10	City of Rancho Palos Verdes, California	\$687,654	\$0	\$0
		<b>Total, Appendix 4</b>	<b>\$77,543,638</b>	<b>\$24,922,433</b>	<b>\$53,241,230</b>

#### 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. DA-06-05	11/04	Crisp County, Georgia	\$190,375	\$190,375
2. DA-08-03	12/07	Ocean Springs, Mississippi	\$102,244	\$102,244
3. DA-09-20	8/09	Harrison County School District, Mississippi	\$375,726	\$375,726
4. DA-10-14	7/10	Hancock County School District, Mississippi	\$610,371	\$610,371
5. DA-16-05	5/05	City of Columbus, Mississippi	\$192,795	\$192,795
6. DA-17-05	6/05	Monroe County School District, Key West, Florida	\$411,026	\$411,026
7. DA-18-05	6/05	City of Owensboro, Kentucky	\$6,128	\$6,128
8. DA-23-04	5/04	Dekalb County, Georgia	\$121,014	\$121,014
9. DD-09-02	12/08	Debris Removal in East Baton Rouge Parish, Louisiana	\$9,749	\$9,749
10. DD-09-03	12/08	Hurricane Katrina Debris Removal Activities in Plaquemines Parish, Louisiana	\$133,253	\$133,253
11. DD-09-04	1/09	City of Kenner, Louisiana, Debris Removal Activities	\$2,550	\$2,550
12. DD-09-13	7/09	City of Muncie, Indiana	\$41,299	\$41,299
13. DD-09-15	9/09	New Orleans City Parks	\$68,140	\$45,687
14. DS-01-05	11/04	City of Los Angeles – General Applications	\$381,864	\$381,864
15. DS-03-06	4/06	Sonoma County, California	\$331,984	\$311,984
16. DS-09-10	8/09	City of Laguna Beach, California	\$17,176	\$17,176
17. INV	4/10 through 9/10	Recoveries as a result of investigations	\$734,063	\$734,063
		<b>Total, Appendix 5</b>	<b>\$3,729,757</b>	<b>\$3,687,304</b>

#### 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<sup>1</sup>

### Contract Audit Reports

Report Category	Questioned Costs	Unsupported Costs	Disallowed Costs
We processed no contract audit reports meeting the criteria of the <i>National Defense Authorization Act for FY 2008</i> during the reporting period April 1, 2010–September 30, 2010	N/A	N/A	N/A

<sup>1</sup> 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 contains additional semiannual reporting requirements pertaining to peer review reports. Federal Inspectors General are required to engage in peer review processes related to both their audit and investigative operations. In keeping with the Section 989C, our office is reporting the following information related to its peer review activities. These activities cover our role as both the reviewed and the reviewing OIG and relate to both audit and investigative peer reviews.

On the audit side, on a 3-year cycle, peer reviews are conducted of an OIG audit organization's system of quality control in accordance with the CIGIE Guide for Conducting External Peer Reviews of the Audit Organization of Federal Offices of Inspector General, based on requirements in the Government Auditing Standards (Yellow Book). Federal audit organizations can receive a rating of pass, pass with deficiencies, or fail.

On the investigative side, quality assessment peer reviews of investigative operations are conducted on a 3-year cycle as well. 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).

### 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 remain open:

- 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 manual, which will be issued in the second quarter of FY 2011.

- DHS OIG emphasize to audit staff the requirement to document the consideration of 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.** Auditors have been notified to better document fraud consideration through training classes and daily supervisory guidance. As an additional control, the Supervisory Review Checklist will be expanded to include the requirement to document consideration of fraud, starting in the audit planning phase when we issue our new manual in the second quarter of FY 2011.

### 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 Audit Operations

DHS OIG conducted a peer review on the Department of Environmental Protection (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.

### Peer Review Conducted by DHS OIG on Other OIG Investigative Operations

DHS OIG conducted a peer review on the U.S. Postal Service (USPS), OIG, Office of Investigations for fiscal year ending September 2008. The USPS OIG Office of Investigations received a peer review rating of "in compliance." No recommendations remain outstanding.

## Appendix 8

# Acronyms

<b>A.D.I.T</b>	Alien Documentation Identification and Telecommunication
<b>AFG</b>	FEMA's Assistance to Firefighters Grant Program
<b>ALJ</b>	Administrative Law Judge
<b>BPA</b>	Border Patrol Agent
<b>Cal EMA</b>	California Emergency Management Agency
<b>CAP</b>	Corrective Action Program
<b>CBP</b>	United States Customs and Border Protection
<b>CBPO</b>	Customs and Border Protection Officer
<b>CEF</b>	Cost Estimating Format
<b>CIGIE</b>	Council of Inspectors General Integrity and Efficiency
<b>CNE</b>	Office of Counternarcotics Enforcement
<b>CO</b>	Correction Officer
<b>COSO</b>	Committee of Sponsoring Organizations of the Treadway Commission
<b>DAE</b>	Disaster Assistance Employee
<b>DAIP</b>	Disaster Assistance Improvement Plan
<b>DCA</b>	Department of Community Affairs
<b>DHS</b>	Department of Homeland Security
<b>DO</b>	Deportation Officer
<b>DOD</b>	Department of Defense
<b>DOJ</b>	Department of Justice
<b>DOL</b>	Department of Labor
<b>DRO</b>	Detention and Removal Operations
<b>EMO</b>	Office of Emergency Management Oversight
<b>EPA</b>	Environmental Protection Agency
<b>FBI</b>	Federal Bureau of Investigation
<b>FEMA</b>	Federal Emergency Management Agency
<b>FINCEN</b>	Finance Center
<b>FISMA</b>	<i>Federal Information Security Management Act</i>
<b>FLETC</b>	Federal Law Enforcement Training Center
<b>GAGAS</b>	Generally Accepted Government Auditing Standards
<b>GOHSEP</b>	Governor's Office of Homeland Security and Emergency Preparedness
<b>GOV</b>	Government-Owned Vehicle
<b>GSA OIG</b>	General Services Administration Office of Inspector General
<b>HMGP</b>	Hazard Mitigation Grant Program
<b>ICE</b>	United States Immigration and Customs Enforcement
<b>ISA</b>	Importer Self-Assessment
<b>ISP</b>	Office of Inspections
<b>IT</b>	Information Technology



## Appendix 8

### Acronyms (continued)

<b>IT-A</b>	Office of Information Technology-Audits
<b>LDHH</b>	Louisiana Department of Health and Hospitals
<b>LSUHSC</b>	Louisiana State University Health Sciences Center
<b>MEMA</b>	Mississippi Emergency Management Agency
<b>MSST</b>	Maritime Safety and Security Team
<b>MWEOC</b>	Mount Weather Emergency Operations Center
<b>NCCIC</b>	National Cybersecurity and Communications Integration Center
<b>NCIS</b>	Naval Criminal Investigative Service
<b>NEMA</b>	Nebraska Emergency Management Agency
<b>NLE</b>	National Level Exercise
<b>NPPD</b>	Nebraska Public Power District
<b>NPSC</b>	National Processing Service Centers
<b>NRF</b>	National Response Framework
<b>NRL</b>	National Research Laboratory
<b>OA</b>	Office of Audits
<b>OCC</b>	Office of Chief Counsel
<b>OCIO</b>	Office of the Chief Information Officer
<b>OGE</b>	United States Office of Government Ethics
<b>OI</b>	Office of Investigations
<b>OIG</b>	Office of Inspector General
<b>OPCSO</b>	Orleans Parish Criminal Sheriff's Office
<b>OPM</b>	Office of Personnel Management
<b>OPR</b>	Office of Professional Responsibility
<b>PA</b>	Public Assistance
<b>PII</b>	Personally Identifiable Information
<b>PW</b>	Project Worksheets
<b>RSD</b>	Recovery School District
<b>S&amp;T</b>	Science and Technology
<b>SMEPA</b>	South Mississippi Electric Power Association
<b>TAA</b>	Trade Agreements Act
<b>TASC</b>	Transformation and Systems Consolidation
<b>TOPOFF</b>	Top Officials
<b>US-CERT</b>	United States Computer Emergency Readiness Team
<b>USCG</b>	United States Coast Guard
<b>USCIS</b>	United States Citizenship and Immigration Services
<b>VIN</b>	Vehicle Identification Number

## Appendix 9

# OIG Headquarters/Field Office Contacts and Locations

### Department of Homeland Security

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

**Telephone Number** (202) 254-4100  
**Fax Number** (202) 254-4285  
**Web site Address** <http://www.dhs.gov/woig/>

#### OIG Headquarters Senior Management Team

<b>Richard L. Skinner</b>	Inspector General
<b>Charles K. Edwards</b>	Deputy Inspector General
<b>Denise S. Johnson</b>	Chief of Staff
<b>Richard N. Reback</b>	Counsel to the Inspector General
<b>Matthew Jadacki</b>	Assistant Inspector General/Emergency Management Oversight
<b>Anne L. Richards</b>	Assistant Inspector General/Audits
<b>Thomas M. Frost</b>	Assistant Inspector General/Investigations
<b>Carlton I. Mann</b>	Assistant Inspector General/Inspections
<b>Frank Deffer</b>	Assistant Inspector General/Information Technology Audits
<b>Charles K. Edwards</b>	Acting Assistant Inspector General/Management
<b>Marta Metelko</b>	Director, Congressional and Public Affairs

## Appendix 9

# OIG Headquarters/Field Office Contacts and Locations (continued)

### Locations of Audit Field Offices

**Boston, MA**

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

**Houston, TX**

Houston, TX 77027  
(713) 212-4350 / Fax (713) 212-4361

**Chicago, IL**

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

**Miami, FL**

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

**Denver, CO**

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

**Philadelphia, PA**

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

### Locations of IT Audits Field Office

**Seattle, WA**

Kirkland, WA 98033  
(425) 250-1363

### Locations of Emergency Management Oversight Office Field Offices

**Atlanta, GA**

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

**New Orleans, LA**

New Orleans, LA 70123  
(504) 739-3938 / Fax (504) 739-3902

**Biloxi, MS**

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

**Oakland, CA**

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

**Dallas, TX**

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

**San Juan, PR**

San Juan, PR 00918  
(787) 294-2530 / Fax (787) 771-3617

## Appendix 9

# OIG Headquarters/Field Office Contacts and Locations (continued)

### Locations of Investigative Field Offices

#### Atlanta, GA

Atlanta, GA 30309  
(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) 775-7492 x239  
Fax: (830) 703-0265

#### 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 York City, NY

Jersey City, NJ 07657  
(201) 356-1800  
Fax: (201) 356-4038

#### Orlando, FL

Orlando, FL 32809-7892  
(407) 804-6399  
Fax: (407) 8804-8730

#### 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

#### Tucson, AZ

Tucson, AZ 85701  
(520) 229-6420  
Fax: (520) 742-7192

#### Washington, DC

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

#### Yuma, AZ

Yuma, AZ 85365  
(928) 314-9640  
Fax: (928) 314-9679

## Appendix 10

# Index to Reporting Requirements

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

Requirement:	Pages
Review of Legislation and Regulations	44-45
Significant Problems, Abuses, and Deficiencies	10-41
Recommendations With Significant Problems	10-41
Prior Recommendations Not Yet Implemented	42-43
Matters Referred to Prosecutive Authorities	Statistical Highlights
Summary of Instances Where Information Was Refused	N/A
List of Audit Reports	52-58
Summary of Significant Audits	10-41
Reports With Questioned Costs	49
Reports Recommending That Funds Be Put to Better Use	50
Summary of Reports in Which No Management Decision Was Made	49-50
Revised Management Decisions	N/A
Management Decision Disagreements	N/A







### **Additional Information and Copies**

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254 4073, fax your request to (202) 254 4305, or visit the OIG web site at [www.dhs.gov/oig](http://www.dhs.gov/oig).

### **OIG Hotline**

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

Call our Hotline at 1 800 323 8603;  
Fax the complaint directly to us at (202) 254 4292;  
Email us at [DHSOIGHOTLINE@dhs.gov](mailto: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.