DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

SEMIANNUAL REPORT TO THE CONGRESS

April 1, 2006 – September 30, 2006

Working Relationship Principles For Agencies and Offices of Inspector General

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

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

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

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

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

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

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

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

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

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

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

Office of Inspector General

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

Homeland Security

October 31, 2006

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

Dear Mr. Secretary:

I am pleased to present our semiannual report, which summarizes the activities and accomplishments of the Department of Homeland Security (DHS) Office of Inspector General (OIG) for the six-month period ending September 30, 2006.

During this reporting period, our office issued 33 management reports (audits and inspections). Our office also issued 29 Gulf Coast hurricane recovery management or advisory reports. In addition, we processed 105 reports on DHS programs that were issued by other organizations. As a result of these efforts, $46 million of questioned costs were identified, of which nearly $14 million were determined to be unsupported. In addition, $74 million of funds that could be put to better use were identified. I am most satisfied, however, with the positive response our reports have received from departmental management. This is demonstrated by the fact that departmental managers have concurred with approximately 90 percent of our recommendations.

In the investigative area, we issued 308 reports. Our investigations resulted in 321 arrests, 333 indictments, and 243 convictions. Our investigators closed 331 investigations and 4,314 complaints were received through the hotline. Additionally, OIG recoveries, fines, restitutions and cost savings totaled approximately $21 million.

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

In closing, I would like to thank all of the hardworking and dedicated professionals in the DHS OIG. As a result of their efforts, we were able to successfully meet the tremendous challenges our office faced during the past six months. Their selfless dedication to

service, oftentimes at the expense of time with family and friends, has not gone unnoticed and is truly commendable.

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

Sincerely,

Richard L. Skinner

Richard L. Skinner
Inspector General

TABLE OF CONTENTS

STATISTICAL HIGHLIGHT OF OIG ACTIVITIES
October 1, 2005 – March 31, 2006

Dollar Impact	
Questioned Costs[1]	$46,365,569
Funds Put to Better Use[2]	$73,531,404
Management Agreement That Funds Be:	
Recovered	$0
De-obligated	$0
Funds Recovered (Audit & Investigative)	$3,255,317
Fines and Restitutions	$901,375
Administrative Cost Savings and Recoveries	$16,396,748
Activities	
Management Reports Issued	33
Gulf Coast Hurricane Recovery Related Reports Issued	29
Investigation Reports Issued	308
Grant and Contract Audit Reports Issued	11
Single Audit Reports Processed	52
Defense Contract Audit Agency	53
Investigations Initiated	658
Investigations Closed	331
Open Investigations	2,517
Investigations Referred for Prosecution	107
Investigations Accepted for Prosecution	138
Investigations Declined for Prosecution	33
Arrests	321
Indictments	333
Convictions	243
Personnel Actions	21
Total Complaints Received	4,314
Total Hotlines Received	4,314
Complaints Referred (to programs or other agencies)	4,394
Complaints Closed	7,584

[1] This amount includes $4,601,431 of questioned costs on contract proposals identified by DCAA and $4,389,862 of questioned costs on single grant audits issued by other organizations according to the *Single Audit Act of 1984*, as amended.

[2] This amount includes $73,500,000 identified by our Office of Gulf Coast Hurricane Recovery, and $31,404 identified by DCAA.

EXECUTIVE SUMMARY

This is the eighth semiannual report to Congress issued by the Department of Homeland Security (DHS) Office of Inspector General (OIG) since its establishment in January 2003. It is issued pursuant to the provisions of Section 5 of the *Inspector General Act of 1978*, as amended, and covers the period from April 1, 2006, to September 30, 2006. The report is organized to reflect our organization and that of DHS.

During this reporting period, we completed significant audit, inspection, and investigative work to promote the economy, efficiency, effectiveness, and integrity of DHS programs and operations. Specifically, we issued 33 management reports (Appendix 3) and 308 investigative reports. Our Gulf Coast Hurricane Recovery office issued 29 hurricane recovery-related reports (Appendix 4). Additionally, we processed 105 reports on DHS programs--53 audits issued by the Defense Contract Audit Agency (DCAA), and 52 single grant audits issued by other organizations according to the *Single Audit Act of 1984,* as amended (Appendix 4). Our reports provide the DHS Secretary and Congress with an objective assessment of the issues, while at the same time providing specific recommendations to correct deficiencies and improve the economy, efficiency, and effectiveness of the respective program.

During this reporting period audits resulted in questioned costs of $46,365,569 of which $13,786,763 was determined to be unsupported costs. In addition, $73,531,404 of funds that could be put to better use were identified. Our investigations resulted in 321 arrests, 333 indictments, and 243 convictions. Moreover our investigators closed 331 investigations and 4,314 complaints received through the hotline. Additionally, recoveries, restitutions, and fines and cost savings totaled $20,553,440.

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

DEPARTMENT OF HOMELAND SECURITY PROFILE

On November 25, 2002, President Bush signed the *Homeland Security Act* (PL 107-296, as amended), officially establishing DHS with the primary mission of protecting the American homeland. On January 24, 2003, DHS became operational. Formulation of DHS took a major step forward on March 1, 2003, when, according to the President's reorganization plan, 22 agencies and approximately 180,000 employees were transferred to the new department.

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

DHS has been reorganized into the following directorates:

Management
Policy
Preparedness
Science and Technology

Other critical components of DHS include:

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

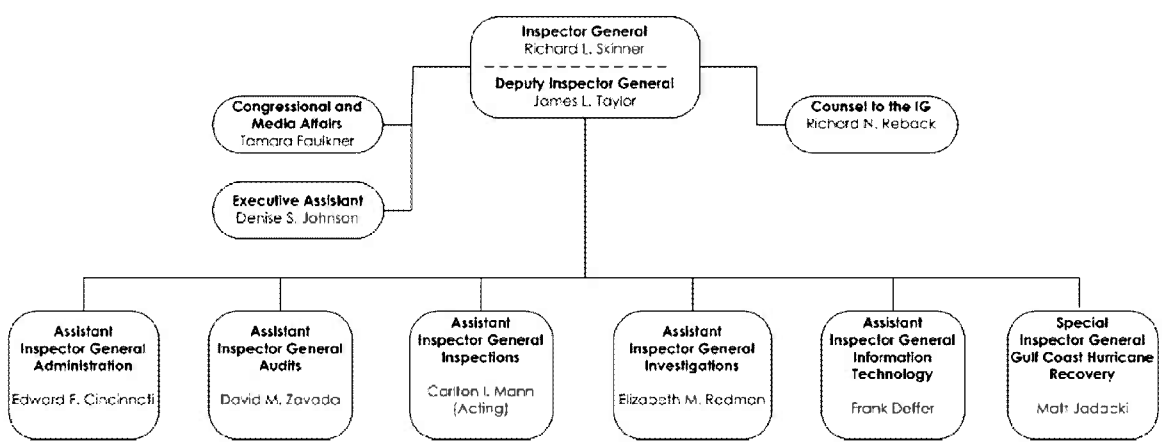
OFFICE OF INSPECTOR GENERAL PROFILE

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

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

We are authorized to have 540 full-time employees. We currently have approximately 100 employees providing audit and investigative oversight of Gulf Coast Hurricane Recovery operations. We are composed of six functional components. We are based in the District of Columbia and have 27 permanent field offices throughout the country. In addition, we have seven temporary field offices dedicated to Gulf Coast Hurricane Recovery oversight operations.

Department of Homeland Security
Office of Inspector General
Management Team



SUMMARY OF SIGNIFICANT OIG ACTIVITY

GULF COAST HURRICANE RECOVERY

Debit Card Overdrafts

Between September 9 and 10, 2005, the Federal Emergency Management Agency (FEMA) issued at least 10,954 debit cards, totaling over $21.9 million, to Hurricane Katrina evacuees located at three shelters in Dallas, Houston, and San Antonio. The cards were provided through the U.S. Debit Card Program by a financial institution acting as financial agent to the U.S. Treasury Department. Each card was initially "loaded" with $2,000. FEMA added money to some of the cards, after the initial $2,000 was loaded, to provide these cardholders with additional assistance. The amount of money added and limitations on its use varied.

In late September 2005, about 284 cardholders had overdrafts, i.e., instances where cardholders received more funds than FEMA authorized. This increased to over 1,400 three months later. By July 2006, over 2,300 cardholders had overdrafts. This represents about 21 percent of the cards issued. On average, based on a 10-month period from October 2005 through July 2006, over 235 additional debit card accounts were being overdrawn each month.

There were a number of reasons why overdrafts occurred. Of $28,433 in overdrafts that we reviewed, miscellaneous point of sale transactions accounted for about 67 percent of the number of overdrafts, but only about 15 percent of the amount overdrawn; car rental agencies and hotels accounted for over 22 percent of the transactions resulting in overdrafts and over 71 percent of the amount overdrawn; and cash withdrawals, although relatively small in number, accounted for almost 14 percent of the total amount overdrawn.

We recommended that FEMA: 1) formalize, through a memorandum of understanding or other appropriate instrument with the U.S. Treasury Department, the terms and responsibilities for resolving overdrafts including the recovery of funds; 2) deactivate all debit cards and accounts as soon as practicable, after providing cardholders written notification; and 3) stop adding funds to debit cards. (GC-HQ-06-51, August 2006)

Review of Hurricane Katrina Activities City of Austin, Texas FEMA Disaster Number EM-3216-TX

The City of Austin received grant awards totaling $44 million from the Texas Division of Emergency Management, a FEMA grantee, for emergency shelter, food, security and interim housing for approximately 3,400 evacuees. The City had an effective system to account for and ensure the appropriate use of disaster grant funds. However, FEMA's award amount exceeded the City's needs by $21.5 million. Also, the City earned interest on the grant funds advanced and had not taken action to dispose of 50 personal computers purchased with grant funds. Federal regulations require subgrantees to remit program income to FEMA and properly dispose of supplies purchased with grant funds.

We recommended that FEMA reduce the grant award by $21.5 million, require the City to remit interest earned, and either recover the remaining value of the 50 personal computers or ensure the City uses the computers for other federally funded programs. (GC-TX-06-32, April 2006)

Management Advisory Report on the Starship Facility Renovation Project, Anniston, Alabama

FEMA spent approximately $7 million to renovate buildings at the abandoned Fort McClellan military base in Anniston, Alabama. The buildings were intended to house up to 660 evacuees from Hurricane Katrina; however, they attracted fewer than 20 residents before their use was discontinued on October 25, 2005. Proper channels of authority were not followed, nor was sound judgment exercised in approving the facility for temporary housing of evacuees from Hurricane Katrina. FEMA officials provided little guidance to the contractor and FEMA's contract oversight was inadequate. Because no written agreement with the administrators of the facility (the Joint Powers Authority) was ever finalized, there was no clear delineation of responsibilities or protection of the Government's interests in the value of the renovations.

We recommended that FEMA: 1) explore legal avenues to recover its investment in the facility; 2) strengthen its management structure over alternative housing for disaster victims, and require that housing officials determine that facilities will be acceptable to evacuees before acquiring them; and 3) require that housing decisions be approved in writing and coordinated with field and headquarters recovery managers. (GC-HQ-06-52, September 2006)

Management Advisory Report on Contract HSFEHQ-06-C-0024 to Provide Assistance to Eligible Evacuees in Need of Housing and Pharmaceuticals

After Hurricane Katrina with its unprecedented displacement of residents, FEMA entered into a contract to reimburse the American Red Cross for the cost of hotel/motel lodging for evacuees. The objectives of the review of the hotel invoices submitted by the American Red Cross to FEMA for reimbursement were to determine whether: (1) lodging rates were reasonable, allowable and necessary; (2) evacuees were eligible to receive lodging; and, (3) contracting practices were effective.

During the review, the American Red Cross notified us that it had identified unallowable charges it billed to FEMA for lodging its employees and volunteers. American Red Cross officials said that they would provide us a weekly update of unallowable charges they identified and they will reimburse FEMA.

We recommended that FEMA determine the extent of the unallowable charges under the lodging contract, initiate collection procedures to recoup unallowable charges from the American Red Cross, and develop and implement controls to identify and prevent future unallowable charges under lodging contracts. A final report will be issued once the review is completed. (GC-HQ-06-41, June 2006)

Review of Hurricane Wilma Activities for Miami-Dade County, Florida FEMA Disaster 1609-DR-FL

Miami-Dade County received an award of $162.9 million from the Florida Department of Community affairs, a FEMA grantee, for debris removal activities associated with Hurricane Wilma. We performed an interim review of costs incurred under the award to determine whether the county (1) was properly accounting for disaster-related costs and whether such costs were eligible for funding under FEMA's public assistance program, and (2) had awarded contracts in accordance with federal procurement standards and had adequate procedures for monitoring the activities of its contractors.

Our review identified $1.5 million of costs that, if claimed by the county, would result in duplicate administrative charges. The county had a policy of retaining 2.25 percent of contractors' invoice billings to help defray the costs of its procurement department. However, in accounting for FEMA project expenditures, the county recorded the full amount of the approved contractor invoices, not the amount actually paid, for eventual billing to FEMA. The 2.25 percent retained from the contractor billings, however, represents costs for administrative activities, which are covered by the statutory administrative allowance received by the county. Moreover, we noted that $72 million of

the $144 million awarded for debris removal activities should be deobligated because final costs would be about 50 percent less than originally estimated.

We recommended that the Director of FEMA's Florida Long-Term Recovery Office, in conjunction with the grantee, (1) inform the county that the 2.25 percent retained from contractor invoices (estimated at $1.5 million) represents duplicate charges that are not eligible for FEMA funding, and (2) deobligate the $72 million in excess funding awarded for debris removal activities. (GC-FL-06-33, April 2006)

Review of Hurricane Wilma Activities, City of Fort Lauderdale, Florida, FEMA Disaster Number 1609-DR-FL

The city of Fort Lauderdale received an award of $24.6 million from the Florida Department of Community affairs, a FEMA grantee, for debris removal activities associated with Hurricane Wilma. We performed an interim review of costs incurred under the award to determine whether the city (1) was properly accounting for disaster-related costs and whether such costs were eligible for funding under FEMA's public assistance program, and (2) had awarded contracts in accordance with federal procurement standards and had adequate procedures for monitoring the activities of its contractors.

Our review identified $1.1 million of unreasonable debris removal contract charges resulting from the improper use of time-and-material contracts. Federal regulations and FEMA guidelines place restrictions on the use of time-and-material contracts because this method of procurement does not provide an incentive for contractors to control costs. Federal regulations allow a grant recipient to use time-and-material contracts but only after a determination has been made that no other form of contracting is suitable and with a contract ceiling price that the contractor exceeds at its own risk. Additionally, FEMA guidelines limit time-and-material contracts for debris removal to a maximum of 70 hours of actual emergency debris clearance.

Despite these restrictions, the city retained 14 contractors using time-and-material contracts and paid them $5.9 million for work that lasted 370 hours, or 300 hours beyond the permissible time limit. Moreover, the contracts were awarded without a determination of whether more suitable contracting arrangements existed and without a ceiling price. We determined that $1.1 million of the contract costs were unreasonable.

We recommended that the Director of FEMA's Florida Long-Term Recovery Office, in conjunction with the grantee, (1) instruct the city, for future declarations, to comply with federal regulations and FEMA guidelines governing contracting practices, and (2) inform the city that $1.1 million of the $5.9 million in time-and-material contract charges represents unreasonable costs that are not eligible for FEMA funding. (GC-FL-06-50, August 2006,)

Reimbursements for Other Needs Assistance Items

FEMA's Other Needs Assistance program includes assistance for personal property, transportation, moving, storage and other expenses. Specifically, the FEMA assistance can be used for the following nonhousing needs: disaster-related medical and dental costs, disaster-related funeral and burial costs, clothing, household items (room furnishings, appliances), tools (specialized or protective clothing and equipment) required for an individual's employment or education, miscellaneous clean-up items (chainsaw, wet/dry vacuum, air purifier, dehumidifier), disaster damaged vehicle, moving and storage expenses related to the disaster, and other necessary expenses or serious needs as determined by FEMA (e.g., generators).

We reviewed payments made to applicants as a result of Hurricanes Katrina, Rita, and Wilma for items qualifying under FEMA's assistance program provision (specifically for chainsaws and generators), and found that controls had not been implemented or were not effective at preventing overpayments. Although proof of payment was required to qualify for reimbursement, payments were being issued to applicants for the maximum allowed amount regardless of the actual cost of the item.

We recommended that FEMA: 1) develop and implement enhancements to the National Emergency Management Information System to ensure that actual purchase amounts are recorded during field inspections and systematically compared to the maximum amounts authorized; 2) review and test system and manual review controls that are in place for those claims processed manually; 3) develop a plan to identify and recoup any future monies issued for amounts greater than actual purchase price or maximum amount allowed, whichever is lesser; and, 4) research and institute a process for assisting those individuals who have legitimate financial hardships but are not able to make the initial purchase for qualifying items. (GC-HQ-06-34, April 2006)

Cannibalization of Travel Trailers by Bechtel

We reviewed an allegation that Bechtel National, Incorporated, one of FEMA's technical assistance contractors responsible for delivering and installing travel trailers in response to Hurricanes Katrina and Rita, was cannibalizing travel trailers at its forward staging area in Mississippi. Our objective was to determine whether the allegation was founded.

We confirmed, through interviews and site visits, that Bechtel did cannibalize 36 travel trailers, and also found other trailers that were not mission capable. Bechtel employees used the cannibalized trailer parts, including batteries, propane tanks and other small items, to repair trailers that were either damaged or not mission capable. Federal Acquisition Regulations and the Bechtel contract require Bechtel to report to FEMA any property that was received in a condition not suitable for its intended use. According to

FEMA officials, Bechtel did not report the damaged travel trailers. However, FEMA also did not inspect the trailers before accepting them into their inventory. Some of the deficient trailers may have been covered under the manufacturer's warranty, but Bechtel's decision to cannibalize damaged trailers may have voided the manufacturer's warranty.

We recommended that FEMA: 1) require the contracting officer's technical representatives to physically inspect contractor storage sites to ensure that contactors report damaged and nonmission-capable trailers, and 2) should determine responsibility for the damaged trailers and take appropriate action to return or repair damaged trailers or recover cost through the warranty. (GC-HQ-06-35, April 2006)

Review of Hurricane Katrina Activities, City of Houston, Texas FEMA Disaster Number EM-3216-TX

Hurricane Katrina displaced over a million people along the Gulf Coast. In Texas, over 400,000 evacuees filled public buildings, convention centers, hotels, and stadiums throughout the state. Local government employees and thousands of volunteers helped provide evacuees with housing, shower facilities, food, clothing, medical care and social services.

The City of Houston received an award totaling $252.6 million from the Texas Division of Emergency Management, a FEMA grantee, for interim housing, project management, and sheltering costs. The award provided 100 percent FEMA funding for as many as 100,000 evacuees living in 34,000 apartment units. The City's disaster-related costs were eligible for funding under FEMA's Public Assistance program; and the City properly accounted for sheltering and project management costs.

However, in the months following the arrival of hurricane evacuees, the City did not properly account for its interim housing costs, representing $222.3 million of the $252.6 million in FEMA funding. Further, the City's efforts to correct its accounting problems led to escalating project management costs. In addition, the City earned approximately $1 million in interest on funds that FEMA advanced to the City.

We recommended that FEMA monitor the City's project management costs to ensure the City only expends funds on approved activities. We also recommended FEMA require the City to remit interest earned on the FEMA funds as required by federal regulation. (GC-TX-06-58, September 2006)

Review of Hurricane Katrina Activities FEMA Disaster No. 1603-DR-LA City of New Orleans, Louisiana Appeal Process for Residential Damage Assessments

The City of New Orleans' Department of Safety and Permits makes determinations of appeals submitted by homeowners related to residential damage assessments performed by the City and their contractors. Damage assessments rated above 50 percent require the homeowner to rebuild under the flood protection requirements of FEMA's National Flood Insurance Program. Of appeals submitted by homeowners with ratings above 50 percent, as a result of Hurricane Katrina, the City lowered the damage ratings to less than fifty percent for the overwhelming majority.

The City did not maintain documentation to support the rating changes for about 95 percent of those ratings that were reduced to below 50 percent during the appeal process. Further, the City did not perform site inspections of the damaged homes, and did not have quality control measures for the appeal process. However, the initial home inspections appeared to have been flawed as well because the inspectors relied on external inspections only and used a questionable rating methodology. Therefore, the accuracy of both the initial inspection process and the appeal process is questionable.

We recommended that FEMA require the City to retain supporting documentation for the appeal process, re-evaluate formulas used for residential inspections, and consider re-inspecting a representative sample of all substantially damaged residences to determine the accuracy of the initial inspections. (GC-HQ-06-53, September 2006)

Review of Hurricane Katrina Activities Congressional Inquiry, Contingency Payment of Contractors in St. Tammany Parish, Louisiana

We received a congressional inquiry regarding an allegation that St. Tammany Parish was not paying its contractors in a timely manner for removing tree limbs damaged by Hurricane Katrina. As a result, the contractors were not paying their subcontractors. The allegation further said that the Parish's reason for not paying was due to their concern that FEMA may not reimburse the Parish for the work. FEMA policy prohibits making contract payments contingent on FEMA reimbursement.

The contract work was substantially complete by March 2006, but the Parish had paid the prime contractor only fifty percent as of early August 2006, and the prime contractor had paid the subcontractors even less than fifty percent of their billings. Parish officials said the payments have been delayed due to their review of the bills for accuracy. However, Parish officials have expressed concern about the eligibility of this work for FEMA reimbursement, and they have not had similar delays in paying for other types of debris removal.

We recommended that FEMA, in coordination with the State and the Parish, encourage the Parish to expedite the review and payment process and ensure that payments to contractors are not contingent upon FEMA reimbursement. (GC-LA-06-57, September 2006)

Review of Hurricane Katrina Activities Dallas Housing Authority, Dallas, TX FEMA Disaster Number EM-3216-TX

The Dallas Housing Authority received an award totaling $29 million from the Texas Division of Emergency Management, a FEMA grantee, to provide approximately 10,800 Hurricane Katrina evacuees with interim housing. The Dallas Housing Authority had an effective system to account for and ensure the appropriate use of disaster grant funds. However, the Dallas Housing Authority earned approximately $206,000 in interest on grant funds advanced by FEMA and generated $37,000 in program income through furniture sales to evacuees. Federal regulations require subgrantees to remit program income to FEMA.

We recommended FEMA require the Dallas Housing Authority to remit program income from interest earned and furniture sales. (GC-TX-06-43, June 2006)

Review of Hurricane Katrina Activities for Magnolia Electric Power Association FEMA Disaster No. 1604-DR-MS

Magnolia Electric Power Association received an award of $10.7 million from the Mississippi Emergency Management Agency, a FEMA grantee, for emergency protective measures and debris removal activities. We performed an interim review of costs incurred under the award to determine whether the association was properly accounting for disaster-related costs and whether such costs were eligible for funding under FEMA's public assistance program.

We determined that the association's grant expenditures included $88,933 of ineligible overtime salary costs for managers and supervisors. On September 9, 2006, after the hurricane and approval of FEMA funding, the association's board of directors modified its overtime policy to make managers and supervisors eligible for overtime pay. This modification authorized overtime pay for the period August 29 to September 25, 2005. However, prior to August 29, 2005, the association's overtime compensation policy prohibited such personnel from receiving overtime pay. Federal cost principles for non-profit associations (U.S. Office of Management and Budget Circular A-122, Attachment A) states that charges to federal grants must be applied consistent with policies and procedures governing both federally-financed and nonfederal activities of an organization. Since the overtime pay modifications were made due to the occurrence of the hurricane and the availability of federal funding, the overtime charges to the FEMA grant for managers and supervisors are ineligible for FEMA funding.

We recommended that the federal Coordinating Officer for Hurricane Katrina in Mississippi, in coordination with the Mississippi Emergency Management Agency, disallow the $88,933 of ineligible overtime costs. (GC-MS-06-49, August 2006)

Improvements Needed in the Review of Classification and Distribution of Hurricane Katrina Disaster Relief Costs

A review of FEMA's procedures for classifying disaster relief costs was conducted as a part of the ongoing oversight of Hurricane Katrina operations. The objective of the review was to determine whether the classification of direct and administrative costs for Alabama, Louisiana, and Mississippi was reasonable and accurate.

FEMA charged direct costs to an administrative cost category resulting in overstated administrative costs and understated direct costs. In addition, FEMA charged costs to the Mississippi disaster that should have been distributed among the three states. Because it did not classify costs properly, FEMA provided inaccurate information to managers, Congress, and the public on how taxpayer funds were spent.

We recommended that FEMA revise the process of classifying costs to accurately identify direct program costs and administration costs, and establish any additional accounts necessary to ensure accurate reporting between administrative costs and direct program costs. In addition, we recommended that FEMA develop a methodology to estimate and distribute costs among states where the goods and services are not state specific. (GC-HQ-06-45, July 2006)

Review of FEMA Policy for Funding Public Assistance Administrative Costs

Currently, FEMA provides assistance in the form of an administrative allowance for public assistance grants, as well as state management administrative grants to cover needs that are unmet by the allowance. A real potential exists for excess funding and a financial windfall for state grantees because the two fund sources cover essentially the same activities and no provisions exist for the state grantees to report or return unused funds granted under the allowance. Funding that the State of Louisiana has available for Hurricane Katrina administrative costs illustrates this point.

The State of Louisiana will receive an administrative allowance of about $24 million based on projected public assistance grants of $4.8 billion. In addition to the allowance, Louisiana also has received a $29 million grant from FEMA for funding a management consultant to supplement the existing state recovery staff. However, the activities funded under the $29 million grant are not limited to those not covered under the allowance,

thereby leaving open the possibility that Louisiana may incur very limited expenses that are covered by the $24 million allowance, creating a windfall to the State.

We recommended that FEMA establish management cost rates to replace both the administrative allowance and state management grants as required by Section 324 of the Stafford Act. In the interim, we recommended that FEMA require states grantees to establish budgets for use of the administrative allowance and require states to submit periodic financial status reports and refund amounts unused under the administrative allowance. (GC-HQ-06-40, April 2006)

Interim Review of Hurricane Katrina Activities, City of New Orleans, Louisiana FEMA Disaster No. 1603-DR-LA Public Assistance Identification

The City received over $102 million in expedited funding to cover emergency protective measures required as a result of Hurricane Katrina. In addition, the City incurred damages relating to debris removal and infrastructure that have been approved for funding by FEMA or are in the review process. FEMA funds these services and damages, if determined eligible under the Public Assistance grant program.

The City's management of its disaster activities was deficient in that its accounting system did not properly allocate costs or document cost eligibility, and the City did not comply with federal contracting procedures. In addition the City did not remit interest earned on the unused portion of the expedited funding.

We recommended that FEMA, in coordination with the State grantee and the City, ensure that the City set up an accounting system that will enable reconciliation of the final claim for specific projects, and that will include only those costs properly allocable and eligible for those projects. In addition, we recommended that contracts not in compliance with federal contracting requirements be amended to ensure compliance, and that the City properly monitor the contracting activities. Finally, we recommended that interest earned on advanced funding be remitted to the federal government as required. (GC-LA-06-56, September 2006)

Interim Review of Hurricane Katrina Activities, St. Bernard Parish Louisiana FEMA Disaster No. 1603-DR-LA Public Assistance Identification Number 087-99087-00

The Parish received over $31 million in expedited funding to cover emergency protective measures required as a result of Hurricane Katrina. In addition, the Parish incurred damages relating to debris removal and infrastructure that have been approved for funding by FEMA or are in the review process. FEMA funds these services and damages, if they are determined to be eligible, under the Public Assistance grant program.

The Parish's management of its disaster activities was deficient in that its accounting system did not allocate costs properly or document cost eligibility, and the Parish did not comply with federal contracting procedures. Also, they did not maintain accountability for capital asset purchases.

We recommended that FEMA, in coordination with the State grantee and the City, ensure that the Parish set up an accounting system that will enable reconciliation of the final claim for specific projects, and will include only those costs properly allocable and eligible for those projects. In addition, we recommended that contracts not in compliance with federal contracting requirements be amended to ensure compliance, and that the City provide additional documentation to support capital purchases or deduct unaccounted for items from their claim. (GC-LA-06-54, September 2006)

Purchase Cards: Control Weaknesses Leave DHS Highly Vulnerable to Fraudulent, Improper, and Abusive Activity

In September 2006, the DHS-IG published a joint audit report with the Government Accountability Office (GAO) regarding DHS' use of the federal purchase card for thousands of transactions related to hurricane relief operations. Inadequate staffing, insufficient training, and ineffective monitoring, along with inconsistent purchase card policies contributed to a weak control environment and breakdowns in specific key controls. DHS needs to enhance documentation that key purchase card internal controls are performed. Based on a statistical sample, GAO and DHS OIG estimated that 45 percent of DHS' purchase card transactions were not properly authorized, 63 percent did not have evidence that the goods or services were received, and 53 percent did not give priority to designated procurement sources. Also, cardholders failed to dispute improper charges, which resulted in losses to the federal government.

The weak control environment and ineffective internal control activities allowed potentially fraudulent, improper, and abusive or questionable transactions to occur. Although we cannot determine the full extent of fraud, waste, and abuse, numerous potentially fraudulent, improper, and abusive or questionable transactions occurred. In addition, poor control over accountable property acquired with purchase cards may have resulted in lost or misappropriated assets. To provide reasonable assurance that fraud, waste, and abuse related to the use of purchase cards is minimized, we recommended that DHS (1) make changes to the draft purchase card manual and issue a final, agency-wide version; and, (2) establish policies and procedures to ensure more effective oversight and enforcement of the purchase card program. DHS concurred with our recommendations. (GAO-06-1117, September 2006, GC)

GULF COAST HURRICANE RECOVERY - INVESTIGATIONS

Our investigators continue to be active participants on the Department of Justice, Fraud Task Force established by the U.S. Attorney General on September 8, 2005. As a result of Hurricanes Katrina and Rita, we have established offices in Baton Rouge, Louisiana, Biloxi, Mississippi, Mobile, Alabama, and Hattiesburg, Mississippi and have staffed these offices primarily with temporary contractor investigators who are Cadre of On-Response Employees or Disaster Assistance Employees. During this reporting period, we conducted 466 investigations, which resulted in 140 indictments, 117 arrests, and 40 convictions. The following paragraphs describe a few examples of Katrina-related investigations initiated through the Hurricane Relief Fraud Hotline and other sources.

False Claims Involving Debris Removal

This is a joint case with the Federal Bureau of Investigation (FBI) involving four individuals who participated in a scheme to file false documentation claiming truckloads of debris that did not exist. Three of the subjects worked for a contractor who was hired to perform work as the county's monitor for the debris removal operations throughout the county. One of their primary responsibilities was to document and approve truckloads of debris that were hauled and disposed of. The fourth individual was a subcontractor who had trucks involved in the debris cleanup. The investigation revealed that the monitors submitted false dump tickets in the subcontractor's name, the subcontractor received payments for these false loads, and the proceeds were split between the individuals. The total amount of the fraud is in excess of $717,000. A federal grand jury indicted each of the four subjects on one count of Title 18 USC § 1001, False Statements and one count of Title 18 USC § 371, Conspiracy. Three of the four subjects have been arrested and no trial date has been scheduled.

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

Our investigation, which was conducted jointly with the U.S. Secret Service, Postal Inspection Service, and Department of Treasury OIG, determined that between September and December 2005, the subject applied for emergency FEMA funds in connection with hurricanes Katrina and Rita, using the names, birth dates, and Social Security numbers of other individuals. As a result of the scheme, FEMA mailed 38 U.S. Treasury checks, made out to the individuals the subject identified, to the subject's motel or to private mailboxes that he rented. The subject then forged the signatures of the payees and deposited the checks into bank accounts that he had opened in the names of other people. On August 28, 2006, the subject pleaded guilty to a three-count information, charging violations of 18 USC § 1344 (*Bank Fraud*), 18 USC § 1341 (*Mail Fraud*), and18 USC § 1957 (*Money Laundering*). Sentencing is scheduled for December 1, 2006.

Three Indicted for FEMA Hurricane Relief Fraud

We conducted an investigation involving suspects who devised a scheme to defraud FEMA by misrepresenting themselves as evacuees from Hurricane Katrina. The false statements resulted in FEMA paying out $33,432 in false claims. On August 30, 2006, a state grand jury indicted three suspects for a state violation of Securing and Executing a Document by Deception.

Hotel Owner Charged With Defrauding FEMA-Update

A joint investigation with the U.S. Secret Service resulted in a 39-count indictment against the owner of a hotel with 22 counts of 18 USC § 1343 (*Wire Fraud)* and 17 counts of filing false claims under 18 USC § 287 (*False Claims*). The owner was arrested and released on a $75,000 bond. The owner is accused of wire fraud and filing false claims totaling at least $232,000 in connection with the disaster relief lodging programs for hurricane evacuees funded by FEMA's Public Assistance Program. A federal magistrate concluded, based upon the testimony of a court-appointed psychiatrist at a hearing, that the defendant was currently incompetent to stand trial.

Two Temporary FEMA employees Arrested-Update

A joint investigation with the FBI resulted in the arrest of two temporary FEMA employees under 18 USC § 201 (*Bribery of Public Officials and Witnesses*) for soliciting bribes from a contractor supplying food for residents displaced by Hurricane Katrina. Both ran a FEMA camp near New Orleans and asked for a $20,000 bribe in exchange for inflating the catering contract.

The two employees pleaded guilty and on August 30, 2006, the first subject received 21 months in prison, 2 years probation, and a $30,000 fine and the second subject received 21 months in prison, 2 years probation, and a $20,000 fine.

Texas Residents Arrested for FEMA Katrina Fraud-Update

A joint investigation with the Department of Labor OIG, the U.S. Postal Service, and the Louisiana Department of Labor has resulted in the arrest of numerous Texas residents under 18 USC § 641 (*Theft of Public Money*) for stealing more than $80,000 in FEMA funds by filing false claims. One resident devised a scheme to impersonate hurricane evacuees and defraud FEMA out of thousands of dollars. She filed the fraudulent claims with FEMA and the Louisiana Department of Labor using the identities, including names and Social Security numbers, of other people, many of them with a similar surname as hers, without their consent. Co-conspirators were arrested on conspiracy charges to

defraud the United States. Between June 1, 2006, and June 26, 2006, twelve subjects pleaded guilty and are awaiting sentencing.

Subject Sentenced for Defrauding FEMA – Update

Our joint investigation with the Department of Labor OIG revealed that a subject filed for and received more than $70,000 from FEMA that the subject was not entitled to receive. The subject was a drug dealer who purchased individuals' biographical information in exchange for drugs. The subject then used the information to file claims for assistance through FEMA and the Louisiana Disaster Unemployment System. The subject pleaded guilty to violating 18 USC § 371 (Conspiracy) and 18 USC § 1708 (*Conspiracy to Commit Wire Fraud*), and was sentenced to 27 months confinement, $17,836 restitution, and 3 years supervised release. (*The original arrest in this case was reported in the SAR for the period October 1, 2005 - March 31, 2006)*

Fugitive Pleads Guilty to Filing False Claim for Disaster Assistance

Our investigation disclosed that the subject, a fugitive who was being sought by the United States Marshals Service on a federal warrant for violating the terms of his supervised release, filed a false claim for Hurricane Rita disaster assistance. The subject claimed that he lived at an address in Beaumont, Texas, during the hurricane when, in fact, the subject was on federal probation in Houston, Texas. As a result of his false claim, the subject received a FEMA registration number and stayed in FEMA-funded hotels while being sought by the U. S. Marshals Service. The subject was arrested by the U. S. Marshals Service in North Carolina and returned to Houston, Texas. The subject pleaded guilty to violating one count of 18 USC § 287 *(Filing a False Claim)*.

Subjects Charged with Filing Multiple False Claims for FEMA Assistance

We conducted a joint investigation with the U. S. Postal Inspection Service, Social Security Administration OIG, and the Small Business Administration OIG, involving two subjects who fraudulently obtained over $48,000 in disaster assistance benefits by filing 39 separate applications, claiming to have suffered damages from hurricanes Katrina and Rita. Following their indictment for violating 24 counts of 18 USC § 1341 (*Mail Fraud*) and six counts of 18 USC § 1028A (*Aggravated Identity Theft*), the subjects were arrested without incident.

Fourteen Charged with FEMA Fraud

We conducted an investigation and found that 14 subjects in Los Angeles used fraudulent addresses and social security numbers to obtain FEMA benefits to which they were not entitled following Hurricane Katrina. Specifically, each of these individuals fraudulently claimed to have resided in Abita Springs, Louisiana, when Hurricane Katrina struck in

August 2005, when they actually resided in Los Angeles. These 14 subjects received 19 FEMA checks totaling $38,716. The Los Angeles City Attorney charged these 14 Los Angeles residents with Grand Theft, a violation of the California Penal Code. Twelve of these individuals were also charged with Conspiracy. To date, 11 individuals have pleaded guilty. Sentences have included up to 30 days in jail, restitution, and community service.

Four Indicted for FEMA Hurricane Relief Fraud

We conducted a joint investigation with the United States Secret Service (USSS) targeting four subjects who knowingly devised a scheme to defraud FEMA by misrepresenting themselves as evacuees from Hurricane Katrina. Their false statements resulted in FEMA paying out $20,425 in false claims. On March 1, 2006, a federal grand jury indicted the four subjects for violations of: 18 USC § 1343 (*Wire Fraud;* 18 USC § 1341 (*Mail Fraud*), and 18 USC § 641 (*Theft of Government Property*). On March 3, 2006, the subjects were arrested pursuant to the indictments. Three subjects pleaded guilty to one count of 18 USC § 1343 (*Wire Fraud*) and the other subject pleaded guilty to one count of 18 USC § 641 (*Theft of Government Property*). Sentencing is pending.

Eleven Indicted for FEMA Hurricane Relief Fraud

We conducted a joint investigation with the FBI and the U.S. Postal Inspection Service that identified numerous subjects residing in Oregon who filed fraudulent FEMA disaster benefit applications following Hurricane Katrina. To date, our investigation has identified 11 subjects in Oregon who were responsible for filing 253 fraudulent Hurricane Katrina applications with FEMA, totaling $470,406 in claims. On October 12, 2005, and on January 27, 2006, the 11 subjects were indicted and arrested for violation of 18 USC § 641 (*Theft of Government Property*). To date, eight suspects have pleaded guilty to one count of 18 USC § 641 (*Theft of Government Property*) and two suspects have pleaded guilty to a total of six counts of 18 USC § 1341 (*Mail Fraud*). Nine suspects have been sentenced to a total of 63 months confinement, 27 years probation, $800 in fines, and $441,184 in restitution. One suspect is awaiting sentencing and one suspect is still at large.

One Indicted for FEMA Hurricane Relief Fraud

We conducted a joint investigation with the Department of Labor OIG, Housing and Urban Development OIG, Social Security OIG, Las Vegas Metro Police Department, the USSS, and the U.S. Postal Inspection Service, which identified approximately 800 suspected fraudulent FEMA applicants residing in the Las Vegas Metropolitan Area. To date, the investigation has identified approximately 50 subjects who were responsible for filing fraudulent Hurricane Katrina applications with FEMA, totaling approximately

$264,000 in claims. On June 5, 2006, a subject was indicted and arrested for violation of 18 USC § 287 (*False Claims*) for participating in a scheme to defraud FEMA by obtaining hotel rooms claiming to have been a victim of Hurricane Katrina, and re-renting the rooms for the purposes of narcotics transactions and prostitution.

Applicant Filed Numerous False Disaster Assistance Claims

Our investigation disclosed that a subject filed 30 claims for disaster assistance using addresses in New Orleans, Louisiana, Pascagoula, Mississippi, Biloxi, Mississippi, and two locations in Alabama. The subject used different social security numbers and different spellings of the first and last names on these claims. Over $277,000 was paid in disaster assistance. A search warrant was conducted on the subject's residence and the majority of the home furnishings were seized. In addition, numerous properties including land were seized. A federal grand jury indicted the subject on 66 counts of fraud against the government. The judge ordered the defendant be detained in custody pending trial.

Multiple Applicants Filed Numerous False Disaster Assistance Claims

This was a joint investigation with the USSS and U.S. Postal Inspection Service where we conducted numerous investigations into fraudulent disaster assistance claims in Florida. The scheme involved a few individuals acting as "brokers" by filing claims for family, friends, and associates, and in some cases receiving a portion of the disaster funds as a commission or fee for filing the claim. The applicants would use false social security numbers and false damaged addresses, usually in the New Orleans, Louisiana area and various locations in east Texas. These claims were filed for hurricanes Katrina and Rita. The 25 individuals who were subsequently indicted and arrested did not live in Louisiana or Texas when the hurricanes made landfall. The total loss to the government as a result of these false claims was approximately $206,000. All but one subject have entered guilty pleas and no trial date has been scheduled for the lone subject awaiting trial.

Applicant Filed False Disaster Assistance Claims

Our investigation disclosed that a subject had filed a claim for disaster assistance claiming to have a primary residence in Gulfport, Mississippi, when in fact the individual was a permanent resident in New York City. The subject received $6,324 in individual assistance and $26,000 was paid by FEMA for hotel rooms occupied by the subject. The subject was indicted by a state district attorney's office on two counts of *Grand Larceny* in the 3rd degree, two counts of *Grand Larceny* in the 4th degree, and one count of *Offering a False Instrument* in the 1st degree. The subject is awaiting trial.

CIVIL RIGHTS AND CIVIL LIBERTIES

We received 78 civil rights and civil liberties complaints from October 1, 2005 to present. Of those, we opened 2 investigations, referred 74 to the Office of Civil Rights Civil Liberties with no response requested, and referred 2 with a 30-day response requested. During the reporting period we did not make any arrests, there were no indictments or convictions and neither of these investigations was resolved.

CUSTOMS AND BORDER PROTECTION

Review of CBP Actions Taken to Intercept Suspected Terrorists at U.S. Ports of Entry

On a typical day, Customs and Border Protection (CBP) processes more than 1.1 million arriving passengers for entry into the country at 324 air, land, and sea ports of entry (POE). It is the responsibility of CBP officers to screen all arriving passengers for customs and immigration violations, and to detect and prevent terrorists and weapons of mass destruction from entering the United States, while simultaneously facilitating legitimate trade and travel. We reviewed procedures employed by CBP to prevent suspected terrorists from entering the United States through the POEs.

CBP has improved information sharing capabilities within the organization to smooth the flow of arriving passengers and increase the effectiveness of limited resources at POEs. CBP procedures are highly prescriptive and withhold from supervisors the authority to make timely and informed decisions regarding the admissibility of individuals whom they could quickly confirm are not suspected terrorists. As CBP has stepped up its efforts to intercept known and suspected terrorists at POEs, traditional missions such as narcotics interdiction and identification of fraudulent immigration documentation have been adversely affected. Inconsistent reporting of encounters with individuals identified on various watch lists is preventing DHS from developing independent intelligence assessments and might be preventing important information from inclusion in national strategic intelligence analyses. Finally, because some CBP officers at POEs have not been granted the necessary security clearance, they are unable to review important information about individuals on watch lists and might not be able to participate with law enforcement agencies in interviews of certain individuals. We made five recommendations, including expansion of a biometric information collection program to include volunteers who would not normally provide this information when entering the United States. (OIG-06-43, June 2006, ISP)

Audit of Payments to the Automated Commercial Environment (ACE) Contractors

CBP is developing the ACE, a new cargo processing system that was initiated to modernize processes for all cargo entering and leaving the United States. In April 2001, CBP awarded the contract to develop ACE to the e-Customs Partnership, headed by the prime contractor, International Business Machines Global Services. As of May 2005, CBP paid e-Customs Partnership over $760 million. ACE is estimated to cost $3 billion and is scheduled for completion in September 2011. The overall objective of the audit was to assess the internal controls related to the review and approval of ACE contractor invoices. Our specific objectives were to determine if procedures, processes, and internal controls were adequate to verify the accuracy, reliability, and completeness of contractor invoices prior to payment, and to review the effectiveness of CBP's process for evaluating the quality of contractor performance in order to determine the amount of award and incentive fee payments.

CBP's management procedures and internal controls for the review and approval of invoices were not adequate. Specifically: (1) CBP did not provide reviewers with sufficient detailed written guidance describing review procedures; (2) reviewers did not always maintain documentation of work performed; and, (3) CBP did not sufficiently research issues identified during reviews. Consequently, there is a risk that CBP might not detect errors or irregularities on the invoices. The internal control process for evaluating the quality of contractor's performance in order to determine the amount of award and incentive fee payments was adequate.

We recommended that CBP streamline and strengthen internal controls over the invoice review process by eliminating redundant invoice review steps performed during the technical and financial reviews; ensuring consistency between reviews of task orders for each cost element; researching the causes of problems noted in the issues logs; periodically monitoring the invoice review process to ensure policies and procedures are followed; and requiring that the activities performed in the review of invoices be documented and retained with the invoice. CBP concurred with our recommendations and took appropriate corrective actions. (OIG-06-66, September 2006, OA)

CBP's Trusted Traveler Systems Using RFID Technology Require Enhanced Security

We audited DHS and select organizational components' security programs to evaluate the effectiveness of controls implemented on Radio Frequency Identification (RFID) systems. Our objective was to determine whether CBP has implemented effective controls to protect critical data processed by its trusted traveler systems. We interviewed personnel at CBP's National Data Center; reviewed applicable DHS and CBP policies and procedures; conducted vulnerability assessments of the databases that collect and process information; and evaluated the effectiveness of physical security and assessed the

security controls over the RFID readers and the RFID-enabled cards and transponders at selected POEs.

CBP has implemented effective physical security controls over the RFID tags, readers, computer equipment, and databases supporting the RFID systems at the POEs visited. No personal information is stored on the tags used for CBP. Travelers' personal information is maintained in and can be obtained only with access to the system's database. Additional security controls would be required if CBP decides to store travelers' personal information on the RFID tags or migrate to universally readable Generation 2 products.

However, CBP has not developed adequate policies and procedures to ensure that security controls are implemented consistently by all POEs to protect its trusted traveler systems. In addition, CBP has not implemented the necessary controls on the system's back end to ensure that the data captured and stored for the trusted traveler programs are properly protected. We also determined that CBP did not ensure that its trusted traveler systems fully comply with all *Federal Information Security Management Act* requirements. For example, the systems reviewed did not have a valid authority to operate, interconnection security and user agreements were not reviewed annually, and security reviews of contractor facilities were not performed.

We recommended that CBP: (1) develop and implement procedures to strengthen user account and password management processes relating to the trusted traveler systems. Procedures should include periodic vulnerability assessments and reviews of all user access; (2) ensure that all vulnerabilities identified, for which risks have not been assumed, be remedied; (3) develop and implement policy and procedures that address security controls over all components of a RFID system; (4) ensure that audit trails are reviewed, documented, and maintained on a regular basis; and, (5) ensure that all *Federal Information Security Management Act* requirements are implemented, including certification and accreditation. CBP concurred with our recommendations and is in the process of implementing corrective measures. (OIG-06-36, May 2006, IT)

Information Technology Management Letter for the FY 2005 Customs and Border Protection Balance Sheet Audit

KPMG LLP performed a review of CBP's information technology (IT) general controls in support of the fiscal year (FY) 2005 CBP consolidated balance sheet audit. The overall objective of this review was to determine the effectiveness of IT general controls of CBP's 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.

In this report, KPMG noted that CBP took corrective action to address prior year IT control weaknesses. Weaknesses relating to entity-wide security and access controls were noted as the most significant issues from a balance sheet audit perspective. Although KPMG noted improvements, many of the conditions identified at CBP in FY 2004 have not been corrected because CBP still faces challenges related to the merging of numerous IT functions, controls, processes, and overall organizational shortages. Collectively, the IT control weaknesses limit CBP's ability to ensure that critical financial and operational data is 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-06-41, June 2006, IT)

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

We audited the strengths and weaknesses of security controls over CBP laptop computers. Our objective was to determine whether CBP had established and implemented adequate and effective security policies and procedures related to the physical security of and logical access to its classified government-issued laptop computers.

To secure CPB data stored on classified government-issued laptop computers, we made three recommendations to the Commissioner, CBP. The Commissioner concurred with our recommendations and has taken or is in the process of taking corrective measures. (OIG-06-64, September 2006, IT)

FEDERAL EMERGENCY MANAGEMENT AGENCY

Audit of the National Urban Search and Rescue Response System

The National Urban Search and Rescue Response (US&R) system is a rapidly deployable federal source for first response to nationwide emergencies, including weapons of mass destruction events. FEMA is responsible for administering the US&R system. After September 11, 2001, Congress provided substantial increases to US&R system funding. Federal preparedness funding for the US&R system reached a high of $65 million in FY 2004, or about 550 percent higher than FY 2001, but fell to $30 million in FY 2005. The audit was performed to determine to what extent FEMA had achieved the US&R system's preparedness goals and to identify opportunities for improvement in US&R system's task force preparedness.

While the US&R system has made improvements, especially in weapons of mass destruction training and equipment preparedness, the task forces fell short in achieving the objectives and standards in three primary areas of readiness: operational, logistical, and management. Systemic deficiencies existed for many of the operational and logistical readiness objectives. Specifically, FEMA did not monitor the task forces' compliance with grant agreement requirements or their achievement of US&R system objectives and standards for optimal task force response preparedness. In addition, FEMA awarded equal grant amounts to each task force without evaluating individual task force readiness or financial needs and did not clearly define program goals. The task forces did not achieve System objectives and standards because of delays in their hiring of full time staff to administer day to day activities, budget constraints, and System management staff shortages. (OIG-06-54, August 2006, OA)

DISASTER GRANT AUDITS

We issued nine grant audit reports valued at about $177 million. Questioned costs for the grant audit reports totaled $36 million, of which $5 million was unsupported. An itemized list of the audit reports that include questioned or unsupported costs are enveloped in Appendix 4.

University of North Dakota, Steam Line, Grand Forks, North Dakota

We audited $28 million in FEMA public assistance funds to the University of North Dakota. The university received $43.9 million in awards for damages caused by severe flooding, severe winter storms, heavy spring rain, rapid snowmelt, high winds, ice jams, and ground saturation due to high water tables that occurred in February through May 1997.

The university did not follow applicable federal procurement standards in awarding $3,005,823 of contracted management service costs. The university procured non-competitive time-and-material cost type contracts for management of the steam line replacement project ($1,836,658) and for the management of reconstruction of 79 buildings ($1,169,165) on its campus. We questioned the entire $3,005,823 (FEMA's share - $2,254,367) because the university awarded the contracts without full and open competition and included cost plus a percentage of cost provisions.

According to 44 CFR 13.37(a)(2), states are responsible for ensuring "that subgrantees are aware of requirements imposed upon them by federal statute and regulation." Further, 44 CFR 13.40 (a) requires states to monitor subgrant supported activities to assure compliance with applicable federal requirements. The University of North Dakota's lack of compliance with federal procurement standards indicates that the university either

ignored or was not aware of federal statutes and regulations and that state officials did not adequately monitor university's subgrant activities.

We recommended the regional director require the North Dakota Division of Emergency Management to develop, document, and implement procedures for future disasters to (a) provide subgrantees timely guidance on federal regulations, standards, and guidelines related to procurement, and (b) monitor subgrantees to ensure compliance with those federal regulations, standards, and guidelines. (DD-08-06, June 2006, OA)

City of Kansas City, Missouri

We audited $26.9 million in FEMA public assistance funds awarded to the city of Kansas City, Missouri by the Missouri State Emergency Management Agency. The city of Kansas City received $28 million in awards for damages resulting from a winter storm that took place on January 29, 2002, with an incident period ending February 13, 2002.

The city of Kansas City did not expend and account for FEMA funds according to applicable federal regulations and FEMA guidelines. The city of Kansas City's failure to competitively bid and properly monitor, record, and substantiate much of the work claimed for this disaster resulted in questioned costs of $9,301,699 (FEMA's share $6,976,274) in claimed costs, consisting of unsupported contractor costs of $4,346,399 (FEMA's share $3,259,799), ineligible costs of $2,019,936 (FEMA's share $1,514,952), unsupported Force Account costs of $1,581,891 (FEMA's share $1,186,418) and unreasonable costs of $1,353,473 (FEMA's share $1,015,105).

Overall, the Missouri State Emergency Management Agency did not perform its grant management responsibilities in an effective manner or according to federal regulations. Further, the city of Kansas City's systems and processes were ineffective in managing and controlling federal funds; and the city of Kansas City did not account for and expend all FEMA funds according to federal regulations and FEMA guidelines. Our recommendations, if implemented properly, would improve the State Emergency Management Agency's grant management, eliminate or reduce the city of Kansas City's noncompliance in future disasters, and recoup $9,301,699 in improperly expended funds for the audited disaster. (DD-09-06, July 2006, OA)

Grand Forks Public School District, Grand Forks, North Dakota

We audited $39.6 million in FEMA public assistance funds awarded to the Grand Forks Public School District by the North Dakota Division of Emergency Management. The school district received an award of $46.5 million for damages caused by severe flooding, severe winter storms, heavy spring rain, rapid snowmelt, high winds, ice jams, and ground saturation due to high water tables during the period February 28, through May 24, 1997.

Overall, the Grand Forks Public School District did not expend and account for FEMA funds according to federal regulations and FEMA guidelines. FEMA's misapplication of the 50 percent rule resulted in the replacement of schools that should have been repaired. The district did not follow federal procurement regulations standards in contracting for a construction management service, which resulted in unreasonable management fees.

The schools claim included questioned costs of $27,396,148 (FEMA's share - $24,656,533), consisting of $23,745,386 (FEMA's share $21,370,847) to replace schools that should have been repaired, unreasonable project management fees of $3,416,855 (FEMA's share $3,075,170), unsupported contract costs of $207,666 (FEMA's share $186,899), and duplicate administrative costs of $26,241 (FEMA's share $23,617). Our recommendations would improve North Dakota Division of Emergency Management's ability to develop, document, and implement procedures for future disasters, provide subgrantees guidance on federal regulations, standards, and guidelines related to procurement, and monitor better subgrantees to ensure compliance with applicable federal regulations, standards, and guidelines related to procurement. It would also recoup $27,396,148 (FEMA's share $24,656,533) in improperly expended funds for the audited disaster. (DD-10-06, August 2006, OA)

Recap of Procurement Problems Identified in Audits of Electric Cooperatives

From September 2002 to January 2006, we issued nine audit reports containing findings that electric cooperatives did not follow federal procurement standards in awarding contracts for utility repairs and debris removal work.[1] As a result, full and open competition did not occur and FEMA had no assurance that contract costs were reasonable. The nine audits covered $59.2 million in electric cooperative subgrantee claims, of which $39.3 million were for costs incurred under noncompetitive contracts.

FEMA grants a substantial amount of federal funding annually to electric cooperatives for natural disasters. For example, FEMA Regions V, VI, VII, and VIII provided $391 million in federal grants to electric cooperatives from 2000 through 2004. We estimate that more than half of that funding reimburses electric cooperatives for costs incurred under contracts that do not comply with federal procurement standards.

Electric cooperatives used noncompetitive, time-and-material contracts without cost ceilings, did not maintain sufficient records for procurement history, and did not perform required cost analyses. These violations occurred because the electric cooperatives either disregarded these procurement standards or were not aware of them. Further, neither the states as grantees nor FEMA, as the responsible federal funding source, enforced the

[1] Includes work of legacy FEMA OIG.

standards when the electric cooperatives submitted their claims for reimbursement of disaster costs.

We have consistently recommended that FEMA regional directors, in conjunction with the states, develop and implement procedures for future disasters to ensure that subgrantees are knowledgeable of and follow federal procurement standards. However, we have seen no improvement in electrical cooperatives' compliance with procurement standards; and FEMA has recovered none of the $10.2 million we questioned in contract costs for the nine audits.

Therefore, we recommended that the Director, FEMA Recovery Division, require all FEMA regional directors to: (1) Provide additional training on federal procurement standards to grantees; (2) require grantees to develop and implement procedures for future disasters to ensure that electric cooperatives are knowledgeable of and follow federal procurement standards; and, (3) require grantees to enforce compliance with federal procurement standards for FEMA public assistance grants to electric cooperatives by disallowing costs incurred under contracts that do not comply with the standards. (DD-11-06, September 2006, OA)

Audit of San Francisco Unified School District, San Francisco, California

We audited public assistance grant funds awarded to the San Francisco Unified School District, San Francisco, California, to determine whether the Unified District expended and accounted for FEMA funds according to federal regulations and FEMA guidelines. The Unified School District received a grant award of $14.7 million from the California Office of Emergency Services, a FEMA grantee, for emergency protective measures, permanent work, and improved project funding for a new administrative building in lieu of repairing the facilities damaged as a result of the Loma Prieta Earthquake that occurred on October 17, 1989. The award provided 75 percent federal funding for 81 projects. The audit covered the period October 17, 1989, to September 30, 2005, and included a review of 11 projects with a total award of $14.4 million. Since the award was not closed until March 2003, the Unified School District was required to retain all necessary records to support its claim until March 26, 2006.

The Unified School District generally expended and accounted for public assistance funds according to federal regulations and FEMA guidelines for 5 of 11 large projects reviewed. However, for six other large projects, we questioned $619,045 in costs claimed by the Unified School District (FEMA's share of the questioned amount is $464,284). The amount questioned consisted of $610,768 (FEMA's share $458,076) in unsupported costs, and $8,277 (FEMA's share $6,208) for duplication of benefits. (DS-02-06, April 2006, OA)

Audit of Sonoma County, Santa Rosa, California

We audited public assistance grant funds awarded to Sonoma County, Santa Rosa, California to determine whether Sonoma County expended and accounted for FEMA funds according to federal regulations and FEMA guidelines. Sonoma County received a grant award of $7.8 million from Office of Emergency Services, a FEMA grantee, for debris removal, emergency protective measures, and repairs to Sonoma County facilities damaged as result of severe winter storms and flooding beginning February 2, 1998, and continuing through April 30, 1998. The award provided 75 percent federal funding for 71 projects. The audit covered the period of February 2, 1998, to June 24, 2003, and included a review of nine projects with a total award of $5,278,824.

We questioned $442,644 claimed by Sonoma County because $361,673 (FEMA's share $271,255) in costs were not adequately supported, $57,853 (FEMA's share $43,390) in costs were ineligible for FEMA reimbursement, $13,050 (FEMA's share $9,788) in credits received by Sonoma County were not provided to FEMA, and $10,068 (FEMA's share $7,550) in costs were covered under FEMA's statutory administrative allowance. FEMA's share of the questioned amount was $331,983. (DS-03-06, April 2006, OA)

Audit of State of Washington's Department of Corrections, Olympia, Washington

We audited public assistance grant funds awarded to the State of Washington's Department of Corrections, Olympia, Washington to determine whether the Department of Corrections expended and accounted for FEMA funds according to federal regulations and FEMA guidelines. The Department of Corrections received an award of $2.0 million from the State of Washington Emergency Management Division, a FEMA grantee, for emergency protective measures and permanent repairs to state prison facilities damaged as a result of the Nisqually earthquake. The incident period was from February 28, 2001, to March 16, 2001. The award provided 75 percent FEMA funding for 27 projects. The audit covered the period from February 28, 2001, to October 31, 2003, and included a review of the two projects totaling $1.8 million at the Washington State Penitentiary in Walla Walla, Washington.

Except for $2,122 (FEMA's share $1,592) in ineligible costs claimed, the Department of Corrections expended and accounted for public assistance funds according to federal regulations and FEMA guidelines. However, the report discusses FEMA's need to develop guidance for identifying and evaluating the eligibility of disaster repairs and the funding of related costs that could have been mitigated if a subgrantee adequately maintained or repaired its facilities prior to a disaster. (DS-04-06, April 2006, OA)

Audit of Los Angeles County Department of Public Works, Alhambra, California

We audited public assistance funds awarded to the Los Angeles County Department of Public Works, Alhambra, California to determine whether the department expended and accounted for FEMA funds according to federal regulations and FEMA guidelines. The department received an award of $29.1 million from Office of Emergency Services, a FEMA grantee, for: debris removal and emergency protective measures; repairs to road, utility systems, water control facilities; and, buildings and equipment damaged by the Northridge Earthquake on January 17, 1994. The award provided 100 percent federal funding for emergency work until January 25, 1994, and 90 percent federal funding thereafter for 195 projects. The audit covered the period January 17, 1994, to May 21, 2004, and included a review of 38 projects with a total award of $19.8 million.

The department's claim included questionable costs of $1,813,454 (FEMA's share $1,632,109). The department also earned $32,509 in interest on federal funds that had not been remitted to FEMA as required by federal regulations. (DS-05-06, July 2006, OA)

Audit of the Contra Costa County, Martinez, California

We audited public assistance grant funds awarded to the County of Contra Costa, Martinez, California to determine whether the Contra Costa County expended and accounted for FEMA funds according to federal regulations and FEMA guidelines. The Contra Costa County received a grant award of $2.2 million from the Office of Emergency Services, a FEMA grantee, for debris removal, emergency protective measures and permanent repairs to the Contra Costa County facilities damaged as a result of the winter storms and flooding that occurred on February 2, 1998. The award provided 75 percent federal funding for 48 projects. The audit covered the period February 2, 1998 to April 7, 2004, and included a detailed review of eight projects with a total award of $1.7 million. In addition, we reviewed the fringe benefits labor costs claimed by the Contra Costa County for all other projects. We questioned a $45,008 in costs claimed by the Contra Costa County. These costs consisted of $19,390 (FEMA's share $14,543) in excessive labor charges and $25,618 (FEMA's share $19,213) in ineligible labor expenses. FEMA's share of the questionable cost was $33,756. (DS-06-06, August 2006, OA)

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

We initiated an investigation after the Internal Revenue Service, Criminal Investigation Division reported that the executive director of a private nonprofit organization was suspected in the theft of federal program funds and submitting false documents to FEMA. Our investigation disclosed that the subject was suspected of submitting over $217,000 in fraudulent claims to FEMA in connection with two disasters. On January 26, 2006, a

multicount indictment was returned charging the subject with violations of 18 USC § 666 (*Theft of Federal Program Funds*), 18 USC §1957 (*Money Laundering*), and 26 USC § 7206 (*Filing False Tax Returns*). **Update:** Subsequent to a trial in federal court defendant was found guilty on a single count of 18 USC § 666 (*Theft of Federal Program Funds*). The defendant was found not guilty on the other counts. Sentencing is scheduled for December 5, 2006.

FEMA Inspector Accused of Soliciting and Accepting Bribes

We conducted an investigation of a FEMA contract inspector who demanded bribes from applicants in exchange for increasing the amount of damage claims submitted to FEMA. The investigation revealed that numerous applicants were approached by the inspector to inflate the amount of damages in return for a kickback of a portion of the award. The inspector was indicted on charges of Title 18 USC § 201(b)(2)(c) *Receipt of Bribes by a Public Official* and 18 USC § 287 *Making False, Fictitious and Fraudulent Claims.* The inspector pleaded guilty to one count of Title 18 USC§ 201(b)(2)(c) and was sentenced to one year and one day of incarceration and ordered to pay restitution.

False Statements and Bribery by City Officials to Steal FEMA Funds

We conducted a joint investigation with the FBI and determined that city officials had filed false claims in order to receive over $90,000 in FEMA assistance. Our investigation determined that the officials then stole approximately $20,000 of the fraudulently obtained funds from city accounts and converted the money to their own use. On April 21, 2006, one official pleaded guilty to a charge of 18 USC § 1001, *(False Statements)* and on May 22, 2006, the other official pleaded guilty to a charge of 18 USC § 666, *Theft or Bribery Concerning Programs Receiving Federal Funds.* Both officials are currently awaiting sentencing.

FEMA Claimant Fraudulently Inflated Damage Claim - Update

We conducted an investigation that found that a claimant had submitted fraudulent damage claims to FEMA following the Cerro Grande Prescribed Fire disaster, which occurred in and around Los Alamos, New Mexico in May 2000. This disaster occurred when the National Park Service initiated a prescribed burn that exceeded the containment capabilities and burned out of control, causing extensive property damage in and around Los Alamos. Following the fire, a Presidential disaster was declared and Congress enacted the *Cerro Grande Fire Assistance Act* to fully compensate victims whose claims were not covered by the Presidential declared disaster. FEMA was designated to administer the *Cerro Grande Fire Assistance Act.* Our investigation determined that a disaster benefit applicant submitted a claim for business damages in excess of $500,000. When the claim was denied and was in the appeal process, the claimant increased the

claim amount to over $750,000. Concurrently, the claimant was under investigation for a $20,000 fraud in community development grants administered by the Department of Energy. As part of a plea agreement, the claimant was indicted on one count of 18 USC § 641 (*Theft of Government Property*). On May 11, 2006, the claimant was sentenced to 36 months probation and ordered to pay $46,808.37 in restitution.

FEMA Temporary Employee in NYC Facilitated $1,000,000 Fraud

A temporary employee of a FEMA Application Support Center was identified as facilitating the submission and approval of false claims for financial assistance to FEMA in the months after the World Trade Center Disaster on September 11, 2001. Our investigation identified 23 fraudulent applications, which resulted in the disbursement of over $1,000,000 in financial assistance. Examination of the documents and bank accounts associated with these disbursements subsequently identified a criminal conspiracy of eight persons responsible for this activity. These persons had generated fictitious identities, counterfeited utility statements to support false claims of residency, and established a mechanism to confirm false claims of employment at nonexistent businesses. This investigation led to the indictment of eight persons on 52 counts charging mail fraud, wire fraud, and filing false claims. Six defendants have pleaded guilty, one is a fugitive, and the remaining defendant has been arrested but is pending judicial action.

IMMIGRATION AND CUSTOMS ENFORCEMENT

A Review of Immigration and Customs Enforcement Discipline Procedures

We conduct quality assurance reviews of the internal affairs units of DHS components. Those reviews examine the handling of allegations, quality and timeliness of investigations, management of the caseload, and reporting of the results. After a review of the internal affairs unit of Immigration and Customs Enforcement (ICE), concerns that some cases were not receiving timely or effective attention were raised. In response to those concerns, the Office of Inspections reviewed ICE's disciplinary system to determine how, once an allegation has been investigated and found to have merit, discipline is imposed and enforced on the offending employee. We studied the timeliness and consistency of disciplinary adjudications, and whether the disciplinary system was being administered uniformly by reviewing 246 cases. We did not assess the reasonableness of the sanctions eventually imposed on ICE employees who engage in misconduct.

Further, we determined that supervisors may, but are not required to ask the Employee and Labor Relations servicing office to assist in assessing an appropriate sanction. However, the Employee and Labor Relations uses five separate Tables of Offenses and

Penalties to guide management in determining appropriate discipline for ICE employees, which has resulted in the inconsistent application of disciplinary action. We made 11 recommendations to improve ICE's ability to establish a single, integrated disciplinary process that is timely and uniform. (OIG-06-57, August 2006, ISP)

Detention and Removal of Illegal Aliens, U.S. Immigration and Customs Enforcement

We conducted an audit of ICE's program for detaining and removing illegal aliens apprehended in the United States and at POEs. The program is administered through ICE's Office of Detention and Removal. The objective of our review was to determine the extent to which the detention and removal office is performing its mission to repatriate all illegal aliens who are removable, including those that pose a potential national security or public safety threat to the U.S.

Currently, the Detention and Removal Office is unable to ensure the departure from the U.S. of all removable aliens. Of the 774,112 illegal aliens apprehended during the past three years, 280,987 (36 percent) were released largely due to a lack of personnel, bed space, and funding needed to detain illegal aliens while their immigration status is being adjudicated. This presents significant risks due to the inability of CBP and ICE to verify the identity, country-of-origin, and terrorist or criminal affiliation of many of the aliens being released. Further, the declining personnel and bed space level is occurring when the number of illegal aliens apprehended is increasing. For example, the number of illegal aliens apprehended increased from 231,077 in FY 2002 to 275,680 in FY 2004, a 19 percent increase. However, during the same period, authorized personnel and funded bed space levels declined by 3 percent and 6 percent, respectively. These shortfalls encourage illegal immigration by increasing the likelihood that apprehended aliens would be released while their immigration status is adjudicated.

Further, historical trends indicate that 62 percent of the aliens released will eventually be issued final orders of removal by the U.S. Department of Justice, Executive Office of Immigration Review and later fail to surrender for removal or abscond. Although the detention and removal office has received additional funding to enhance its Fugitive Operations Program, it is unlikely that many of the released aliens will ever be removed. As of December 30, 2005, there were more than 544,000 released aliens with final orders of removal who have absconded.

We recommended that the Assistant Secretary of ICE develop a plan to provide ICE with the capacity to: (1) detain and remove high-risk aliens; (2) intensify its efforts to develop alternatives to detention; and, (3) resolve with the State Department issues that are preventing or impeding the repatriation of illegal aliens who are not of Mexican origin. Also, we are recommending that the Office of Detention and Removal expedite its efforts to implement a data management system that is capable of meeting its expanding data

collection and analysis needs relating to the detention and removal of illegal aliens. Such a system would significantly enhance the detention and removal office's ability to support future budget requests, identify emerging trends, and assess its overall mission performance. (OIG-06-33, April 2006, OA)

Former Prison Captain Guilty Of Civil Rights Violation and Witness Tampering

A former prison captain was convicted in federal court on February 8, 2006 for civil rights violations and three counts of tampering with witnesses. Specifically, the defendant was convicted of one count of 18 USC § 242 (*Deprivation of Rights Under Color of Law*) and three counts of 18 USC § 1512 (*Witness Tampering*). The captain was indicted in April 2004 for beating an immigration detainee. The indictment resulted from a joint investigation with the U.S. Department of Justice, Civil Rights Division, the FBI, and the U. S. Attorney's Office regarding the subject's use of excessive force on the detainee. On June 28, 2006, this former prison captain was sentenced to 32 months confinement and 24 months supervision upon his release from prison.

Immigration Enforcement Agent Indicted for Harboring Fugitive

We advised an immigration enforcement agent that an acquaintance of hers was wanted for *Unlawful Flight to Avoid Prosecution.* The agent denied having any knowledge of the fugitive's whereabouts. We later discovered the agent and the fugitive together at the fugitive's temporary residence. The agent was arrested and charged with violating 18 USC § 1071 *(Concealing a Fugitive from Arrest)*. The agent resigned from her position.

Former ICE Special Agent Convicted of Worker's Compensation Fraud

A former ICE special agent pleaded guilty to falsely receiving $239,000 in federal worker's compensation benefits. The employee claimed that an on-the-job injury left the employee unable to work and therefore entitled to receive federal worker's compensation benefits. Investigation disclosed that the employee, while receiving worker's compensation benefits, was working for another company and that the employee failed to report the income. In addition, the employee made false statements that caused his worker's compensation payments to continue. The subject was indicted on three counts of violating *Title 18 USC§ 1920, (Fraud Related to Worker's Compensation Benefits*). The subject was arrested, has entered a guilty plea, and is awaiting sentencing.

ICE Special Agent in Charge is Arrested and Charged with Exposing Himself in Public

We initiated an investigation based upon the arrest by local authorities of an ICE special agent in charge who allegedly exposed himself to a juvenile female at a shopping mall. The investigation revealed that the special agent in charge had, in fact, exposed himself in

front of the juvenile female. The special agent was charged with and subsequently pleaded guilty to one count of a state statute, *Exposure of Sexual Organs,* and sentenced to one year of supervised probation. The special agent in charge retired from ICE following the incident.

Retired Immigration Inspector Convicted Of Workman's Compensation Fraud

A cross check by the Department of Labor of workman's compensation recipients and wage earners identified a retired U.S. Immigration and Naturalization Service employee as receiving both. Joint investigation by this office and the Department of Labor identified the suspect and confirmed his disability retirement in December 1994 from the U.S. Immigration and Naturalization Service where he had collateral duties as a workman's compensation specialist. Our investigation determined that the retired inspector had drawn combinations of tax-free workman's compensation and retirement annuity from 1994 until 2003 while being employed in a private sector job. The former employee pleaded guilty to *"a Criminal Information"* charging him with embezzlement. He was sentenced to six months in custody, followed by two years of supervised release, and ordered to make restitution in the amount of $120,689.

Death of an ICE Detainee

We conducted an investigation into the circumstances surrounding the death of a detainee who died while in ICE custody at a county contract facility. Our investigation confirmed that the detainee's cause of death was suicide, and that some ICE policies and procedures governing the handling of potentially suicidal ICE detainees were not adhered to by contract employees.

ICE Agent Pleads Guilty to Bribery

We conducted an investigation after receiving information from an agent of ICE who had been offered a bribe from an illegal alien seeking to avoid deportation. We arranged for several undercover meetings which resulted in documentation of the bribe including the receipt of $5,000 in bribe money. The subject was arrested and, on May 23, 2006, entered a guilty plea to violation of 18 USC § 201, *(Bribery of a Public Official).*

Border Patrol Agent Pleads Guilty to Accepting Bribes and Selling Identity Documents

We conducted a joint investigation with the FBI into allegations that a border patrol agent was involved in drug and alien smuggling. On three occasions, a confidential informant bought immigration and identity documents from the subject—documents that the subject had obtained in the course of his official duties. The subject agreed to assist in facilitating drug smuggling by guaranteeing the safe passage of two kilograms of cocaine through a

border patrol checkpoint in exchange for $5,000. On June 27, 2006, the subject was arrested for violating 18 USC § 201 (*Bribery of Public Officials and Witnesses*). On August 22, 2006, a superseding indictment added three counts of 18 USC § 1028 (*Unlawful Use or Transfer of Identification Documents*). On September 7, 2006, the subject pleaded guilty to the aforementioned charges. Sentencing is pending.

Marked Bribe Payment seized from residence of the Border Patrol agent

Immigration and Customs Enforcement Detention Facility Not Negligent in Death of Detainee

A Cuban national alien detained by ICE at a contract facility operated by Corrections Corporation of America died while in custody. The detainee was incarcerated pending deportation to Cuba. A review of all aspects of the incident was conducted with the cooperation of ICE, the Corrections Corporation of America, and the Department of Health and Human Services, Public Health Service. Our investigation determined that the detainee's civil rights were not violated and that the death was not the result of misconduct or wrongdoing by any employee of ICE or the Corrections Corporation of America.

United States Border Patrol Chief Patrol Agent Improperly Issued I-94s with the Assistance of his Deputy

We conducted an investigation and determined that a United States Border Patrol chief border patrol agent misused his position and abused his authority by improperly issuing arrival-departure record documents (I-94s) to three aliens. Our investigation revealed that the chief patrol agent issued I-94s to an illegal alien and to an aggravated felon shortly after the September 11, 2001, terrorist attacks with the assistance of his deputy. The chief patrol agent resigned in lieu of a proposed termination and the deputy chief patrol agent was demoted to a non-supervisory position.

Border Patrol Agent Pleads Guilty to Possession of a Machinegun and Possession of Unregistered Firearms

In a joint investigation with the FBI, ICE, and CBP, we determined that a previously arrested border patrol agent who was on pretrial release for violating 18 USC § 922(a)(6), (*False Statement During Firearms Purchase)*, and 18 USC § 922(d)(2), (*Disposing of Firearm to Prohibited Person)*, was still in possession of prohibited weapons. After a search of the subject's residence disclosed several illegal weapons, including a firearms silencer, a 9mm caliber machinegun, and two sawed-off shotguns, he was charged in a superseding indictment with five additional weapons-related violations. On September 6, 2006, the subject pleaded guilty to violating 18 USC § 922 (*Possession of a Machinegun*), and three counts of violating 26 USC § 5861 (*Possession of an Unregistered Firearm*). Sentencing is pending.

ICE Officer arrested for Online Solicitation of a Minor

We conducted a joint investigation with the State Attorney General's Office, Cyber Crimes Unit involving a subject involved in internet crimes. Investigation found that the officer transmitted obscene material to a minor. The officer was charged with *Online Solicitation of a Minor,* and *Criminal Attempt Sexual Performance by a Child* in violation of a state penal code. The officer is incarcerated awaiting trial.

Subject Charged in Reverse Bribe

We conducted an investigation involving an attempted bribe of a public official. The subject, while "on-duty" status, offered a federal officer approximately $300 for each undocumented aliens he allowed into the United States from Mexico. An undercover investigation resulted in the arrest of the subject. Subject was charged for violation of Title18 USC § 201 (*Bribery of a Public Official*) and 8 USC § 1324 (*Smuggling and Transporting Aliens*). The subject waived her right to a grand jury and pleaded guilty to "*a Criminal Information"*. Subject is pending sentencing.

Border Patrol Agent Arrested for Aggravated Sexual Assault

A joint investigation with a District Attorney's Office-Special Operations Group resulted in the arrest of a United States border patrol agent. The arrest was based on an indictment in state grand jury charging the agent with *Sexual Assault* and *Aggravated Sexual Assault* in violation of a state penal code. The investigation determined that the border patrol agent, while off-duty, took a female to his apartment and gave her an unknown drug that rendered her unable to resist his advances. As a result, the border patrol agent was

charged with having sexual relations with the female without her consent. The border patrol agent is currently on bond pending judicial proceedings in state district court.

CBP officer Arrested for Bribery and Alien Smuggling

We conducted an investigation after receiving information that a CBP officer was working with a Mexican-based alien and drug smuggling organization. The case was investigated jointly with the local Border Corruption Task Force. The investigation disclosed that the CBP officer knowingly allowed vehicles containing illegal aliens and marijuana to enter the United States. On numerous occasions, the smugglers rented vehicles in the United States, drove them into Mexico, loaded them with aliens and marijuana and returned to the United States through the CBP officer's inspection lane. The investigation disclosed that one of the smugglers reportedly gave the CBP officer a Lexus sports utility vehicle, and there were numerous unexplained deposits into the CBP officer's bank account. In June 2006, the CBP officer and seven co-conspirators were indicted and arrested on charges of 18 USC § 201 (*Bribery*); 18 USC § 371 (*Conspiracy*); 8 USC § 1324 (*Alien Smuggling*); 21 USC § 952, 960 (*Importation Of Marijuana*); 21 USC § 841(*Possession Of Marijuana With Intent To Distribute*); 18 USC § 2 (Aiding *And Abetting*); 26 USC § 7206 (*Filing a false tax return*); and 18 USC § 981 (Civil forfeiture) and 18 USC § 982 (Criminal forfeiture); and, Title 28 USC §2461 (*Criminal forfeiture*). Approximately $36,500 in cash was seized along with two vehicles. Three of the co-conspirators have pleaded guilty to 18 USC § 371 (*Conspiracy*); 8 USC § 1324 (*Alien Smuggling*); and 26 USC § 7206 (*Filing a False Tax Return).* The remaining co-conspirators are pending trial.

Supervisory CBP officer Arrested for Alien Smuggling

We conducted an investigation after receiving information from a source that a U.S. resident alien was smuggling illegal aliens into the United States with the help of a corrupt CBP officer at a POE on the Southwest border. Our investigation, which was conducted jointly with the Border Corruption Task Force, found that this CBP officer was working for an alien smuggling organization and receiving thousands of dollars for every vehicle containing illegal aliens he allowed to enter the United States without proper inspection. In June 2006, the CBP officer and two alien smugglers were arrested for violation of 8 USC § 1324 (*Alien Smuggling*). Trial dates are pending.

Border Patrol Agents Sentenced for Alien Smuggling – Update

We conducted an investigation of two border patrol agents who were allegedly involved in alien smuggling. We conducted this investigation jointly with the Drug Enforcement Administration Narcotic Task Force and found that the two border patrol agents were working for an alien smuggling organization. In August 2005, the two border patrol agents were arrested and charged with violations of 8 USC § 1324 (*Alien Smuggling*).

Additionally, our investigation revealed that one of the border patrol agents was an illegal alien. He was further charged with violations of 18 USC § 922 *Alien in Possession of a Firearm* and 18 USC § 911 *False Claim to U.S. Citizenship*. One of the border patrol agents pleaded guilty to 8 USC § 1324 (*Alien Smuggling*) for his role in conspiring to smuggle 99 illegal aliens into the country; and 18 USC § 911 *False Claim to U.S. Citizenship*. On July 28, 2006, he was sentenced to 60 months imprisonment.

Impersonating a DHS/Federal Officer – Using Fraudulent Documents to Purchase Firearms

We conducted an investigation upon learning that an individual had allegedly used fraudulent DHS law enforcement identity documents to purchase firearms at a discount price. Our case was investigated jointly with the ICE, California Department of Justice, Inland Empire Task Force. Our investigation found that the subject had purchased numerous firearms while using the fraudulent documents. In July 2006, the subject was indicted on seven counts of *Possession of False Identity Documents and Impersonating an Officer* of the United States. Subsequent searches revealed that the subject had multiple firearms in his possession. Trial is scheduled for September 2006.

Supervisory Border Patrol Agents Arrested for Bribery and Alien Smuggling – Update

We conducted an investigation of two supervisory border patrol agents after receiving information that they were working for an alien smuggling organization. Our investigation determined that the two border patrol agents had been working with the alien smuggling organization since 2003 and that they had facilitated the entry of illegal aliens into the United States, released illegal aliens and drivers of the alien smuggling organization from immigration custody and facilitated the travel of illegal aliens further into the U.S. Our investigation found that the two border patrol agents told alien smugglers about ongoing investigations concerning their smuggling organizations in exchange for cash. It is estimated that the agents earned $900,000. On March 9, 2006, the

two border patrol agents were arrested and charged with: 8 USC § 1324 (*Alien Smuggling*); 18 USC § 371 (*Conspiracy*); 18 USC § 201 (*Bribery*); 18 USC § 1001 (*False Statements*); 18 USC § 2 (*Aiding and Abetting*); and, 26 USC § 2206 (*Filing a False Tax Return*). On July 7, 2006, both agents pleaded guilty to charges of 18 USC § 201 (*Bribery*) and 26 USC § 2206 (*Filing a False Tax Return*). One border patrol agent forfeited $100,300 and the other forfeited $85,940. Sentencing is scheduled for September 29, 2006.

Operator of Mobile Car Wash Business Convicted of Fraudulent Scheme and Artifice

Our investigation disclosed that the owner of a mobile car wash business hired to wash border patrol vehicles at various sector stations had fraudulently overcharged the border patrol more than $23,000 for car washes. The owner of the business, who had a previous embezzlement conviction and was paying $29,000 in restitution, had agreed to charge $20 per vehicle. However, he later used a portable credit card swipe machine to begin charging the border patrol $200 for some of the car washes, instead of $20. The subject pleaded guilty to one count of *Fraudulent Scheme and Artifice*, a Class 2 Felony, in a state court for the 116 fraudulent charges he made to the border patrol from January 2004 through November 2004. The subject was sentenced to four years in prison and ordered to pay restitution in the amount of $23,570.

Border Patrol Employee Indicted for Theft of Union Funds

We conducted a joint investigation with the U.S. Department of Labor, Office of Labor-Management Standards, into the theft of funds from the American Federation of Government Employees by a border patrol employee. On at least two occasions, the employee used the American Federation of Government Employees funds to pay her personal credit card expenses and fees. On July 13, 2006, a grand jury indicted the employee on two counts of "*Theft*", a class three felony under a state statute. A trial date is pending.

Smuggling of Contraband into ICE Detention Facility Disrupted

We investigated allegations that contract security guards employed at a particular ICE processing center for housing illegal aliens were introducing contraband into the facility for profit. The illegal contraband included alcohol, cigarettes, and controlled substances. An undercover investigation was initiated, which lead to the arrest and conviction of one contract security guard after agreeing to deliver a quantity of marijuana to an inmate and accepting a bribe payment. The investigation identified four other contract guards as being involved in the ring. Though insufficient evidence existed to charge the other guards with criminal offenses, the investigation did produce sufficient evidence to have three of the contract guards removed from the facility. The fourth guard was removed due to an unrelated matter.

MANAGEMENT

Buy American Act Compliance

House of Representatives Conference Report H.R. 109-79 for *DHS Appropriations Act, Fiscal Year 2006* directed the OIG to audit DHS' compliance with the *Buy American Act*.

The *Buy American Act* was enacted in 1933 to encourage the federal government to buy from American companies. Since then, Congress has modified the law—adding numerous exemptions and trade agreements that permit the federal government to purchase foreign products from other countries.

In our review of contracts, we noted no significant *Buy American Act* compliance issues. Our contract review included looking at a sample of contracts from the FY 2005 foreign purchase reports, contracts awarded during FY 2005, and contracts shown in the Homeland Security contract information system as having foreign countries of origin. Contracts reviewed totaled $199 million; Act compliance exceptions represented less than one percent of contracts reviewed.

We could not, however, determine whether DHS complied with the *Buy American Act* requirements on a comprehensive, agency-wide level because of system limitations and manual reporting errors. We identified these same problems in a June 2005 OIG report, in which we recommended DHS provide *Buy American Act* training, complete implementation of automated contract writing systems, improve automated reporting systems for tracking *Buy American Act* compliance, and continue manual data collection requirements until these systems are improved. DHS agreed with the recommendations in our June 2005 report and continues to implement corrective actions; therefore, we made no additional recommendations in this report. (OIG-06-37, May 2006, OA)

Special Report: Letter on TSA's FY 2005 Financial Statements

We engaged the independent public accounting firm KPMG LLP to audit the Transportation Security Administration's FY 2005 financial statements. TSA did not provide final financial statements on which KPMG could report; therefore, KPMG did not complete the audit. This marked a significant departure from TSA's past performance in preparing auditable financial statements. The previous statements received unqualified opinions.

During the period of their engagement, however, KPMG noted certain matters involving internal control and other operational matters at TSA. Other matters may have been

identified had KPMG been able to perform all procedures necessary to express an opinion on the TSA FY 2005 financial statements. Of the matters identified by KPMG, our office recommended that TSA give prioritized attention to: accounting treatment of fees; financial reporting; financial systems security; grants monitoring and year-end accounting; undelivered orders, contract file maintenance, and letters of intent accrual; and, obligation recoveries. (OIG-06-48, July 2006, OA)

Audit of DHS' Corrective Action Plan Process for Financial Reporting – Report No. 1

During 2006, DHS initiated a formal corrective action plan effort aimed at developing corrective action plans and tracking specific milestones for its material internal control weaknesses. As part of this effort, DHS developed a detailed automated tracking system to monitor corrective action plan progress. The audit was performed by KPMG LLP and focused on assessing the process and guidance that DHS has put in place and the overall progress in developing a department-wide corrective action plan.

We recommended that DHS enhance its process and guidance by further emphasizing management's responsibility for internal control and move away from a disproportionate reliance on external audits; providing additional tools for analyzing the "root cause" of internal control deficiencies; better integrating corrective action plans with other related management assessment and corrective action plan initiatives; and establishing clearer accountability for completing corrective actions. We also recommended greater coordination with corrective action plans being developed and implemented to address IT weaknesses. Similarly, roles and responsibilities of responsible officials and accountability need to be clear and coordinated. (OIG-06-52, July 2006, OA)

Audit of DHS' Corrective Action Plan Process for Financial Reporting – Report No. 2

KPMG LLP performed an audit of the DHS' progress in developing specific corrective action plans for four internal control weaknesses prioritized for improvement in FY 2006. These weaknesses were financial management oversight; financial reporting; accounting for Fund Balance with Treasury; and accounting for actuarial liabilities. These weaknesses are primarily attributable to three entities within DHS: Office of the Chief Financial Officer, ICE, and the United States Coast Guard (USCG).

Overall we identified well-developed corrective action plans at ICE and some progress at the Office of the Chief Financial Officer. We reported very little progress in developing effective corrective action plans at USCG.

Office of the Chief Financial Officer: During FY 2006, the Office of the Chief Financial Officer demonstrated some progress in initiating a department-wide corrective action

plan process and taking steps to more actively monitor progress. We recommended that further analysis of "root causes" be performed and detailed corrective action tasks with time sensitive milestones be developed, assigned for completion, and validated.

ICE: ICE proactively began its corrective action plan process in the first quarter of FY 2006. Consequently, they are further along in developing and executing corrective action plans than the other DHS entities. We found the corrective action plans were comprehensive and well developed. To further improve their corrective action plans, we recommended that ICE better define the criteria used to determine when a corrective action is complete and integrate the validation process with control testing planned for conducting management's OMB Circular, A-123 Management's Responsibility for Internal Controls.

USCG: USCG's plans were general in nature and lacked adequate detail. Underlying root causes were limited to only those previously identified through the financial statement audit. Consequently, the corrective action plans did not include a fully developed and detailed list of tasks to correct weaknesses, a timeframe for completion, or adequate accountability. We made specific recommendations related to all key elements of the USCG's plans. Our primary recommendations were for the USCG to perform a thorough root cause analysis of weaknesses, to include financial systems, processes, and human resources, and to develop a detailed list of tasks and milestones. We also recommended the USCG make a realistic assessment of the resources required to plan and execute corrective actions. (OIG-06-61, September 2006, OA)

DHS Management of Automated Procurement Systems Needs Improvement

We audited the DHS Office of the Chief Procurement Officer to determine the effectiveness of the IT systems used to oversee Hurricane Katrina-related procurements. We also performed a limited review of internal control processes associated with information security as well as capital planning and investment control requirements. This audit included a review of applicable DHS policies, procedures, and other appropriate documentation.

We recommended that the DHS Office of the Chief Procurement Officer establish a process 1) to ensure that procurement information is entered accurately into "Federal Procurement Data System –Next Generation" within three days of the contract award; 2) discontinue the use of DHS contract information system as a feeder system to federal procurement data system –next generation; and, 3) update the DHS acquisition manual to be consistent with government-wide procurement policy guidance. We also recommended that the DHS Chief Procurement Officer coordinate with the DHS Chief Information Officer to: 1) develop the required interconnection security agreements for DHS' contract-writing systems and have them signed by the appropriate designated

approving authority; and, 2) develop an appropriate cost-benefit analysis prior to the selection of an enterprise-wide contract-writing system.

The DHS Office of the Chief Procurement Officer concurred with three of our five recommendations and has advised us on the actions that DHS will take to correct these deficiencies. However, DHS disagrees with our recommendations 1 and 3. (OIG-06-46, July 2006, IT)

Information Technology Management Letter for the FY 2005 DHS Financial Statement Audit

KPMG LLP performed a review of DHS' IT general controls in support of the FY 2005 DHS financial statement engagement. The overall objective of this review was to determine 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 2005, KPMG continued to find IT general control weaknesses at each bureau. 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 is maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively impact the internal controls over DHS' financial reporting and its operation, and KPMG considers them to collectively represent a material weakness under standards established by the American Institute of Certified Public Accountants. (OIG-06-49, July 2006, IT)

Additional Guidance and Security Controls Are Needed Over Systems Using RFID at DHS

We audited DHS and its organizational components to evaluate the effectiveness of controls implemented or planned on systems using RFID technology. Further, for systems utilizing RFID technology that were in the planning stages, we determined whether security controls were adequately addressed during the system development process. We performed our audit at four DHS organizational components: Science and Technology (S&T), TSA, CBP, and the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program. Our results were summarized in separate reports with findings and recommendations issued to CBP, TSA, and US-VISIT. No report was issued to S&T as its efforts in RFID technology involved only systems in the early stages of development.

CBP, TSA, and US-VISIT have implemented effective physical security controls over RFID tags, readers, computer equipment, and databases supporting the RFID systems at the sites visited. No personal information is stored on the tags. Sensitive information is maintained in and can be obtained only with access to the system's database. Additional security controls would be required if any component decides to store sensitive or personal information on RFID tags or migrates to universally readable Generation 2 products.

Overall, good physical security controls exist on the RFID systems we audited. However, there remain other concerns that should be addressed to help improve system security. DHS needs to develop policy and procedures regarding RFID technology, incorporating security planning while in system development, and strengthen database security controls. CBP, TSA, and US-VISIT need to determine whether the necessary database security controls are being implemented in their RFID systems. Processes need to be put in place at the department level to ensure that database security concerns at all DHS components are addressed and mitigated.

We recommended that the DHS Chief Information Officer: (1) develop and implement policy and guidance that addresses security controls for systems being implemented using RFID technology; (2) direct the DHS RFID Coordination Group to finalize its charter and ensure that all components using or planning to use RFID technologies are represented in the group; and (3) ensure that components adhere to DHS information security procedures for all systems using RFID technology. DHS agreed and plans to take steps to implement each of the recommendations. (OIG-06-53, July 2006, IT)

Survey of DHS Data Mining Activities

We surveyed the DHS to identify and describe data mining activities used to support the counterterrorism mission. Data mining and advanced analytics are evolving technologies that assist in the discovery of patterns and relationships from vast quantities of data. Data mining employs techniques from statistics, machine learning, database management, and visualization. These techniques aid the work of analysts, agents, and investigators and provide knowledge in a manner that aids and informs decision-makers. While various definitions of data mining exist, for the purpose of our survey we defined data mining in a manner to broadly illustrate the range of applications and tools that DHS uses to assist its personnel with knowledge discovery, predictive modeling, and analytics.

We identified 12 systems and capabilities that DHS personnel use to perform data mining activities to support DHS' mission of counterterrorism. Nine systems are operational and three systems are under development. While these data mining activities may perform various processes, we categorized and arranged our descriptions in a way that describes selected data mining processes and tools ranging from basic to advanced analytical tasks.

The categories include expert systems, association processes, threat and risk assessment tools, collaboration and visualization processes, and advanced analytics. (OIG-06-56, August 2006, IT)

Evaluation of DHS' Information Security Program for Fiscal Year 2006

We conducted an independent evaluation of the DHS' information security program and practices in order to comply with the Office of Management and Budget's *Federal Information Security Management Act of 2002* reporting requirements. We evaluated DHS' progress in implementing its agency-wide information security program. In doing so, we specifically assessed DHS' plan of action and milestones as well as its certification and accreditation processes.

In response to a United States House of Representatives, Committee on Appropriations report, DHS implemented a department-wide remediation plan in order to certify and accredit all operational systems by the end of FY 2006. The completion of this plan will eliminate a major factor that held DHS back from strengthening its security program in prior years.

In addition, some of the issues that we identified and recommendations that we made in our FY 2005 report to assist DHS and its components in the implementation of its information program have been addressed. Some of the measures taken include developing a process to maintain a comprehensive inventory and increasing the number of operational systems that have been certified and accredited.

Despite several improvements in DHS' information security program in the past year, DHS components, through their information systems security managers, have not completely aligned their respective information security programs with DHS' overall policies, procedures, and practices. For example, all DHS systems have not been properly certified and accredited; all components' information security weaknesses are not included in a plan of action and milestones; data in the enterprise management tool, *Trusted Agent Federal Information Security Management Act*, is not complete or current; and, system contingency plans have not been tested for all systems.

While DHS has issued substantial guidance designed to create and maintain secure systems, we identified areas where the implementation of agency-wide information security procedures require strengthening: (1) certification and accreditation; (2) plan of action and milestones; (3) security configurations; (4) vulnerability testing and remediation; (5) contingency plan testing; (6) incident detection, analysis, and reporting; and, (7) specialized security training. (OIG-06-62, September 2006, IT)

OFFICE OF INSPECTOR GENERAL

Office of Inspector General Laptop Computers Are Susceptible To Compromise

The results and recommendations concerning OIG classified laptops are summarized in a classified report and not mentioned here.

We audited DHS and its organizational components' security controls over select government-issued laptop computers, including our own operations. We employed many essential security controls for our sensitive but unclassified and classified laptops. Specifically, we developed a standard configuration for our sensitive but unclassified laptops, as well as procedures to patch and update sensitive but unclassified laptop computers that are routinely connected to our network. Further, we established adequate physical security measures for our laptops and have implemented many of the security program requirements for our classified system that contain our laptops and desktops. Our network includes sensitive but unclassified laptops and desktops.

We need to further strengthen our configuration, patch, and inventory management controls necessary to protect our government-issued laptop computers. Specifically, we have not: (1) implemented a standard configuration, that meets required minimum-security settings for sensitive by unclassified laptops; (2) established effective procedures to patch laptop computers that are not regularly connected to the OIG network; (3) maintained an accurate inventory; (4) cleared sensitive data from laptops prior to reuse within the organization; and, (5) applied the appropriate classification labels or markings. In addition, we noted a number of concerns regarding our classified laptops.

We recommended that our Assistant Inspector General for Administration work closely with our Chief Information Officer to: (1) remedy the existing critical vulnerabilities in the standard configuration for sensitive but unclassified laptops, and determine whether similar vulnerabilities and remediation are relevant to all government-issued computers; (2) establish procedures to ensure that model systems are configured to protect our data and are verified prior to implementation; (3) develop procedures to ensure that all of our laptops are patched and updated in a timely manner; (4) implement an enterprise property management system to ensure an accurate laptop inventory is maintained, and that all laptop computers are handled according to our inventory management policies and procedures; (5) clear or sanitize laptop computers before reissue or disposal, and ensure that all laptops are labeled appropriately; and, (6) develop a risk assessment for our network, test our contingency plan, and provide specialized privacy training to relevant officials.

In addition, this report contains a classified appendix. To secure our data stored on classified government-issued laptop computers, we made three recommendations to our

Assistant Inspector General for Administration. We have taken, or are in the process of taking, corrective measures in response to each recommendation. (OIG-06-58, August 2006, IT)

OFFICE OF INTELLIGENCE AND ANALYSIS

Evaluation of DHS' Security Program and Practices For Its Intelligence Systems For Fiscal Year 2006

We conducted an evaluation of Top Secret/Sensitive Compartmented Information systems under the DHS' purview. According to the *Federal Information Security Management Act* requirements, our evaluation focused on DHS' information assurance posture, including the policies and procedures in place for DHS' intelligence systems. We performed our work at the program and organizational component levels, focusing on the system security controls for a select sample of intelligence systems, according to the requirements in *Director of Central Intelligence Directive 6/3, Protecting Sensitive Compartmented Information Within Information Systems.*

The objective of our evaluation was to determine whether DHS is adequately and effectively protecting top secret/sensitive compartmented information and the systems that support DHS' intelligence operations and assets from unauthorized access, use, disclosure, disruption, modification, or destruction. As part of our evaluation, we conducted detailed system security vulnerability assessments of eight of DHS' intelligence systems and evaluated DHS' privacy policies as they apply to intelligence systems.

Overall, we noted that DHS formally established the Office of Intelligence and Analysis to implement their IT security program for its intelligence systems and assets. However, issues exist with coordinating and managing the security program for DHS' intelligence systems. We also identified issues regarding the certification and accreditation of its intelligence systems; plan of action and milestones process; incident detection, handling procedures, reporting, and analysis process; and information security training and awareness program for employees with significant responsibilities for DHS' intelligence systems. (OIG-06-59, August 2006, IT)

OFFICE OF OPERATIONS COORDINATION

Homeland Security Information Network Could Support Information Sharing More Effectively

State and local personnel have opportunities and capabilities not possessed by federal agencies to gather information on suspicious activities and terrorist threats. By working together, the various levels of government can maximize the benefits of information gathering and analysis to prevent and respond to terrorist attacks. The *Homeland Security Act of 2002* assigned responsibility to DHS to coordinate the federal government's communications relating to homeland security with state and local government authorities, the private sector, and the public. To meet this mandate, DHS is implementing the Homeland Security Information Network (HSIN).

The objectives of this review were to (1) identify DHS' plans and activities for sharing information with state and local governments; (2) determine how well HSIN supports these plans and activities; and, (3) identify challenges to information sharing among federal, state, and local government agencies.

Due to time pressures, DHS did not complete a number of the steps essential to effective system planning and implementation, hindering the success of the HSIN system. Specifically, DHS did not clearly define its HSIN's relationship to existing collaboration systems and also did not obtain and address requirements from all HSIN user communities in developing the system. In addition, DHS did not adequately evaluate each of its three major HSIN releases prior to their implementation. Further, DHS has not provided adequate user guidance, including clear information sharing processes, training, and reference materials. Without establishing a baseline and developing specific performance measures, DHS has no effective way to track or assess information sharing using HSIN.

As a result of these system planning and implementation issues, HSIN is not effectively supporting state and local information sharing. Although users generally like the web portal technology because of its user-friendliness and flexibility, those we interviewed said they are not committed to the system approach. Users are confused and frustrated, without clear guidance on HSIN's role or how to use the system to share information effectively. Because some lack trust in the system's ability to safeguard sensitive information, and because the system does not provide them with useful situational awareness and classified information, users do not regularly use HSIN. Instead, users resort to preexisting means such as related systems and telephone calls to share information, which only perpetuates the ad hoc, stove-piped information-sharing environment that HSIN was intended to correct. Resources, legislative constraints,

privacy, and cultural challenges—often beyond the control of HSIN program management—also pose obstacles to its success.

We made several recommendations for the Director, Office of Operations Coordination to ensure effectiveness of the HSIN system and information sharing approach. Communication of HSIN's mission and vision is needed to clarify its relationship to other federal systems. Also, clear information-sharing guidance, standard operating procedures, manuals, and training are needed to describe what and how information should be shared, and to define the intelligence data flow for users. Additionally, broad stakeholder involvement in business and system requirements determination should be encouraged. Lastly, adequate information-sharing measures should be identified and used to track HSIN effectiveness. In response to our report, the acting director of the Office of Operations Coordination concurred with our recommendations in their entirety. The acting director further said that the recommendations were solid, and when implemented, would improve the effectiveness of the HSIN system and information sharing. (OIG-06-38, June 2006, IT)

PREPAREDNESS

Progress in Developing the National Asset Database

We assessed the actions DHS has taken to identify and organize the nation's critical infrastructure and key resources in the national asset database.

The methodology for populating the national asset database was limited and subjective, leading to an inaccurate and incomplete representation of the nation's assets. The varying presence of non-critical assets confirmed that the national asset database is not an accurate depiction of the nation's critical infrastructure and key resources, and significant variation in state-provided assets prevented comparing one state or sector to another in any comprehensive analysis. Substantial work remains for the DHS in developing the data and the risk assessments tools to analyze the assets before the national asset database can support the management and resource allocation decision-making envisioned in the national infrastructure protection plan. We recommended four specific actions to the Under Secretary for Preparedness to improve the development and quality of the national asset database. (OIG-06-40, June 2006, ISP)

GRANT AUDIT REPORTS

We issued two grant audit reports valued at nearly $55 million. Questioned costs for the grant audit reports totaled $712,285, of which $606,154 was unsupported. An itemized list of the audit reports with questioned or unsupported costs is included in Appendix 4.

The Commonwealth of Virginia's Management of State Homeland Security Grants Awarded During Fiscal Years 2002 and 2003

The Office for Domestic Preparedness awarded about $53.5 million to the Commonwealth of Virginia from the FY 2002 State Domestic Preparedness Program, and from Parts I and II of the FY 2003 State Homeland Security Grant Program. Cotton & Company, under a contract with DHS OIG, conducted the audit to determine whether the Commonwealth: (1) effectively and efficiently implemented the first responder grant programs; (2) achieved the goals of the programs; and, (3) spent funds in accordance with grant requirements.

The audit determined that the Commonwealth could improve its grant performance by: (1) adequately documenting its homeland security plan and implementing the grant programs; (2) allocating Office for Domestic Preparedness grant funds based on its risk assessment or stated needs and goals; and, (3) effectively monitoring local jurisdictions. The audit also determined that the Commonwealth did not have adequate internal controls over monitoring cash advances and did not adhere to grant requirements regarding equipment purchases. The audit questioned $471,768 in costs claimed by the subgrantees visited. (OIG-06-45, July 2006, OA)

Audit of Grant 2004-TK-TX-0003 and 2005-GH-T5-0001 Awarded to the National Domestic Preparedness Coalition of Orlando, Florida

The Office of Domestic Preparedness awarded the National Domestic Preparedness Coalition of Orlando, Florida, $654,383 under grant number 2004-TK-TX-0003 and $405,816 under grant number 2005-GH-T5-0001. These grants provided funding to demonstrate and evaluate the DHS comprehensive assessment model developed by the coalition to perform comprehensive vulnerability assessments for communities and community leaders. The Office of Domestic Preparedness approved a grant performance period of March 2004 to August 2004 for the 2004 grant, and a performance period of June 2005 through May 2006 for the 2005 grant.

The National Domestic Preparedness Coalition of Orlando, Florida, did not account for grant funds in accordance with federal regulations and grant guidelines because its claim consisted of $134,386 in unsupported labor costs, $16,861 in overstated operating and administrative expenses, and $1,500 in unallowable travel costs. As a result, we questioned $152,747 in costs for these specific categories. In addition, the coalition did not credit the grants for $87,770 in licensing fee reimbursements it received from its software developer. We also reported that the coalition needed to improve its grant management procedures regarding: (1) the preparation and submission of financial status

reports; (2) cash management; and, (3) compliance with grant requirements for travel. We questioned a combined total of $240,517 in costs. (OIG-06-34, May 2006, OA)

SCIENCE & TECHNOLOGY

Improved Administration Can Enhance Science and Technology Laptop Computer Security

We audited the DHS and its organizational components' security program to evaluate the security and integrity of select government-issued laptop computers. This report focuses on the S&T. Our objective was to determine whether S&T has established and implemented adequate and effective security policies and procedures related to the physical security of and logical access to government-issued laptop computers.

Significant work remains for S&T to further strengthen the configuration, patch, and inventory management controls necessary to secure its data stored on government-issued laptop computers. Specifically, S&T has not established: (1) a standard configuration that meets required minimum-security settings, for its laptops; (2) effective procedures to patch laptop computers that do not regularly connect to the network or that were released without a standard image; and, (3) adequate inventory management procedures. As a result, sensitive information stored and processed on S&T's laptop computers may not be protected adequately. Further, because S&T uses the same procedures to develop a model for its laptop and desktop computers, the configuration weaknesses identified with laptop computers are relevant to all government-issued computers assigned within S&T.

S&T officials stated that they have already taken or plan to take corrective action to address many of the weaknesses we identified, including the implementation of an updated standard configuration for the laptops at one of the S&T field offices reviewed. As our fieldwork was complete, we did not verify that the weaknesses had been remedied.

We recommended that the Under Secretary for S&T instruct the S&T Chief Information Officer to: (1) remedy the existing critical vulnerabilities in the standard model configuration for laptops. Further, the S&T Chief Information Officer should confirm whether similar vulnerabilities and remediation are applicable to all S&T issued computers; (2) ensure that the updated model system is correctly implemented; (3) develop procedures to ensure that all S&T laptops are patched and updated in a timely manner; and, (4) implement appropriate inventory management controls, including effective inventory reviews, physical security controls, and classification labeling. (OIG-06-42, June 2006, IT)

Improved Administration Can Enhance Science and Technology Classified Laptop Computer Security

We audited DHS and its organizational components' security programs to evaluate the security and integrity of select government-issued laptop computers. We assessed the strengths and weaknesses of security controls over S&T laptop computers. Our objective was to determine whether S&T had established and implemented adequate and effective security policies and procedures related to the physical security of and logical access to its classified government-issued laptop computers.

To secure S&T data stored on classified government-issued laptop computers, we made three recommendations to the Under Secretary for S&T. The Under Secretary concurred with our recommendations and has taken or is in the process of taking corrective measures. (OIG-06-63, September 2006, IT)

TRANSPORTATION SECURITY ADMINISTRATION

Review of TSA Non-Screener Administrative Positions

The Chairman, House Aviation Subcommittee, raised concerns that TSA's administrative staff was top-heavy and underutilized at several airports, and included overpaid supervisory screeners. The staff of 1,850 employees supports a passenger and baggage-screening workforce of 47,037 screeners. We determined that TSA's initial staffing actions lacked coherency and resulted, in some cases, in significant disparities in staffing at airports. Additionally, TSA had never determined the precise number of federal security director administrative positions it needs. TSA has completed a plan to reallocate employees at the airports identified to be proportionately over- and under-staffed. TSA expected to complete implementing the plan by September 30, 2006.

We did not recommend a cap or limit on TSA's administrative positions. We made four recommendations which included conducting a workforce analysis of the federal security director non-screener staff and developing a staffing model to identify the number of employees actually needed at airports. (OIG-06-65, September 2006, ISP)

Transportation Security Administration Continuity of Operations Program

Continuity of Operations (COOP) planning is the means by which federal departments, agencies, and their subcomponents ensure that their mission-essential functions continue under all circumstances. We audited TSA's COOP program to determine whether TSA has a viable COOP capability and a COOP plan that meets government-wide

requirements and guidance that defines a viable COOP capability; and whether TSA and DHS provide effective guidance and oversight over TSA's COOP plan and program.

TSA's ability to continue its mission-essential functions during a variety of emergencies is at risk due to the lack of a comprehensive and effective COOP plan and program. The TSA headquarters COOP plan and program only partially address the 11 required elements that define a viable COOP. Without a complete and viable COOP plan, TSA's ability to support, coordinate, and direct intermodal transportation security during an emergency could be impaired or fail.

In addition, through FEMA its lead component on COOP matters, DHS has provided only limited oversight of TSA COOP activities. It has not assessed the extent to which TSA, as well as other DHS components, are maintaining a current COOP plan and program that contains all the required information.

We made recommendations to TSA and FEMA to take appropriate steps to ensure that TSA implements a comprehensive and effective COOP plan and program. TSA and FEMA concurred with our recommendations. TSA noted progress made in the COOP program since the end of our fieldwork. FEMA stated that the agency does not currently have the authority to serve as a regulatory agent responsible for ensuring that agencies have a viable COOP program in full compliance with Federal Preparedness Circular 65. (OIG-06-60, August 2006, OA)

Review of the Transportation Security Administration (TSA) Collection of Aviation Security Service Fees

The *Aviation and Transportation Security Act*, Public Law 107-71, established passenger and air carrier security fees to reimburse TSA for its costs of providing air passenger and property security services at the nation's airports. The Act required TSA to impose a uniform passenger civil aviation security service fee (passenger security fee) on passengers of domestic and foreign air carriers whose flights originated in the United States. The Act also allowed TSA to impose an aviation security infrastructure fee on air carriers. During FY 2004, TSA collected $1.6 billion in passenger security fees and $283 million in aviation security infrastructure fees. The audit evaluated TSA monitoring controls, oversight, and air carrier collection and remittance of passenger security fees and at the request of TSA, evaluated calendar year 2000 passenger and property screening expenses reported by air carriers to determine the accuracy or reasonableness of the costs reported by the air carriers.

For passenger security fees, TSA had not developed adequate controls and until late 2004, had not conducted audits to oversee the accuracy of the air carriers' collection and remittance practices. As a result, TSA did not know that the three air carriers reviewed did not identify, collect, and remit $2.7 million in fees for the period covered during the

audit. For the calendar year 2000 passenger and property screening expenses, serious problems existed with data accuracy, integrity, and reliability. Based on our work at TSA, national airports, property- and passenger-screening contractors, and the air carriers, we estimated that unremitted aviation security infrastructure fee amounts from program inception to March 2005, totaled about $49 million. During our audit, the GAO, as mandated by the *2005 Homeland Security Appropriation Act*, initiated a review to evaluate the reasonableness of the $319 million aviation security infrastructure fee amount used by TSA as the maximum reimbursement from the air carriers. Its April 2005 report estimated that aviation security infrastructure fee collections should be between $425 million and $471 million. Our report was consistent with GAO's findings and highlights similar concerns with the integrity and reliability of the calendar year 2000 expenses reported by the air carriers in FY 2002. (OIG-06-35, May 2006, OA)

TSA's Development of Its Weapons Management System Using RFID

We audited DHS and select organizational components' security programs to evaluate the effectiveness of controls implemented on RFID systems. TSA is developing a weapons management system using RFID in the Federal Air Marshal Service's (FAMS) Federal Flight Deck Officer program. While the system is in the first of three phases of development, we noted security weaknesses that should be addressed and corrected prior to the system being fully implemented.

Based on our interviews with TSA personnel and review of applicable documentation, we noted that: (1) the system has not been included in the TSA system inventory; (2) the system has not been certified and accredited; (3) some security controls were inadequate; and, (4) TSA has not developed a RFID policy to ensure that security controls are implemented to protect its systems using this technology.

We recommended that TSA: (1) ensure that its weapons management system is included in its system inventory and an authority to operate is granted for each phase of development; (2) all appropriate security controls, based on DHS information security procedures and configuration guides, should be implemented; and, (3) develop, implement, and distribute an RFID policy that addresses security controls over all components of an RFID system. TSA agreed and has already taken steps to implement each of the recommendations. (OIG-06-44, July 2006, IT)

DHS Must Address Significant Security Vulnerabilities Prior To TWIC Implementation

We audited the information security management and access controls implemented for the systems supporting the transportation worker identification credential program prototype phase. Our audit objective was to determine whether adequate system security

controls have been implemented on transportation worker identification credential systems to protect sensitive and biometric data from unauthorized access, use, disclosure, disruption, modification, or destruction. Our audit work was based on direct observations; vulnerability and wireless system security scans; and an analysis of applicable transportation worker identification credential documents. In addition, we interviewed TSA, the United States Citizenship and Immigration Services (USCIS), and selected port management officials and security personnel.

We recommended that TSA: (1) establish a formal structure for the effective oversight and management of security for the transportation worker identification credential program; (2) timely remediate system and configuration management vulnerabilities; and, (3) revise and develop necessary security documentation and standard operating procedures that are essential to attain a robust security posture for the transportation worker identification credential program prior to full implementation. TSA concurred with and has already taken steps to implement the recommendations. (OIG-06-47, July 2006, IT)

TSA Baggage Screener Arrested For Structuring Money

This was a joint investigation with the Internal Revenue Service, Criminal Investigation Division involving a TSA employee who attempted to evade the reporting requirements by structuring over $80,000 in cash that he obtained in Germany and brought into the United States. The investigation disclosed that the employee reportedly obtained money from a fiancé in Germany and then brought the money into the United States and used the money to purchase land and a house. The employee was indicted for evading the reporting requirements in violation of Title 31 USC § 5313(a). The employee was arrested and is awaiting trial.

TSA Screeners Confess to Thefts from Passenger Baggage

We conducted an investigation into thefts occurring at the screening checkpoints at a U.S. international airport. Two screeners confessed to stealing thousands of dollars in United States currency, as well as jewelry and other items. The screeners were indicted and subsequently arrested on charges of Title 18 USC § 371 *Conspiracy* and 18 U.S.C. § 641 *Theft of Government Property*. Both screeners were terminated as a result of this investigation. Each screener was sentenced to 1 year probation, 100 hours of community service and $600 restitution.

TSA Employee Arrested on Charges of Internet Child Pornography

We conducted a joint investigation with local authorities into the activities of a TSA employee who was alleged to have engaged in soliciting a minor for sexual acts and providing pornographic material to a minor. The investigation revealed that the employee

had engaged in internet "chats" with an individual he believed to be a 14-year-old female, but was, in fact, an undercover detective. We executed a federal search warrant at the employee's residence to recover pornographic materials from the computer. The employee was subsequently arrested and charged locally with 16 counts of Florida State Statutes *FSS; Transmission of Harmful Material to a Minor and 7 counts of FSS; Use of a Computer to Seduce a Child.* The employee resigned from TSA.

Six TSA Screeners Arrested for Lying about Prior Arrests on their Security Forms

Our investigation disclosed that six TSA screeners failed to disclose prior criminal histories to the TSA before being hired by the agency. Six screeners were arrested and charged with violating 18 USC § 1001 *(False Statements)*. To date, three of the subjects have pleaded guilty to making false statements on official government documents.

TSA Supervisory Security Screener Sentenced for Distributing Explicit Material to a Minor

We conducted a joint investigation with a state bureau of investigation into an allegation that a TSA supervisory security screener was communicating through the Internet with an undercover agent whom he believed to be a 13-year-old girl. The undercover agent was a state special agent and communicated with the TSA supervisory security screener from April 17, 2005, to August 29, 2005. On August 31, 2005, the TSA supervisory security screener was arrested and charged with a State Penal Code (*Sending Harmful Matter to Minor by Telephone Messages, Electronic Mail, Internet, or Commercial Online Services*). In January 2006, this screener voluntarily resigned from TSA. On March 29, 2006, the former screener pleaded *Nolo Contendere* to two counts of violating a state Penal Code, *(Distribution or Exhibition of Lewd Material to a Minor via the Internet, or Commercial Online Services)* and was sentenced to 365 days in jail on a work furlough program. The former screener was also placed on five years of formal probation and required to register as a convicted sexual offender.

TSA Security Screeners Charged with Theft

We conducted an investigation into allegations that four TSA security screeners were targeting Japanese tourists and stealing Japanese Yen from their checked luggage. In March 2005, one of the screeners was caught stealing 196,168 in Japanese Yen ($1,800 US) from a passenger's checked luggage. A second TSA security screener was implicated and surrendered 123,000 in Japanese Yen ($1,100 US) that he had stolen from checked luggage. Two additional TSA security screeners have been identified. All four TSA security screeners have been placed on unpaid administrative leave. On March 3, 2006, two of the screeners were charged with violations of 18 USC § 641 (*Theft of Government Property*); 18 USC § 659 (*Theft of Carrier Shipments*); 18 USC § 371

(*Conspiracy*); and, 18 USC §654 (*Employee of the United States Converting Property of Another*). On April 18, 2006, these two screeners pleaded guilty to one count of 18 USC § 654 (*Employee of the United States Converting Property of Another*). Their sentencing is pending. Prosecution of the other two screeners is pending.

Summons Issued for TSA Screener and Her Boyfriend

We conducted an investigation regarding a TSA screener who smuggled a controlled substance into a federal correctional institute and provided it to her inmate boyfriend. Prior to being employed by TSA, the subject had worked for the Federal Bureau of Prisons. On July 18, 2006, the United States Magistrate issued a summons for both subjects for violations of Title 18 USC §1791 (*Providing or Possessing Contraband in a Prison*). A trial date is pending.

FEDERAL AIR MARSHAL SERVICE

Federal Air Marshals (FAMs) Sentenced for Bribery and Distribution of Cocaine – Update

A joint investigation with the FBI led to the arrest, guilty plea, and sentencing of two former FAMs who sought, received, and accepted bribe money from a confidential informant seeking the safe passage of 15 kilograms of cocaine through the aviation transportation system. Each pleaded guilty to violating 18 USC § 201 (*Bribery of Public Officials and Witnesses*) and 21 USC § 841 (*Unlawful Manufacture, Distribution, or Possession of a Controlled Substance*). On August 28, 2006, a United States district judge sentenced one of the former FAMs to 87 months in federal prison, and the other to 108 months in federal prison. The lesser sentence was a result of the court's consideration of one of the former FAM's cooperation with the United States. (*The original arrests in this case were reported in the Semiannual Report to Congress for the period October 1, 2005 - March 31, 2006)*

Federal Air Marshal Pleads Guilty to Theft of Government Money; Second FAM resigns

We initiated an investigation after discovering altered hotel lodging receipts during a search incident to arrest in a separate investigation involving corrupt FAMs. The investigation disclosed that two other FAMs were involved in travel voucher fraud. One of the subjects resigned during the investigation. On June 15, 2006, the second subject pleaded guilty to violating 18 USC § 641 (*Theft of Government Money*), and agreed to resign from FAMS. Sentencing is pending.

Federal Air Marshal Sentenced for Child Pornography Offense

Our investigation disclosed that a FAM received, possessed, produced, and distributed computer images of child pornography. While in jail awaiting trial, the subject contacted minor children by telephone and by handwritten letters. We conducted an additional investigation into those allegations and discovered that the content of the letters and telephone conversations were sexual in nature. The subject pleaded guilty to violating 18 USC § 2252(a) (*Relating to Possession, Manufacture, and Receipt of Child Pornography*), and was sentenced to 20 years confinement, lifetime reporting as a sexual offender, and three years supervised release.

UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES

U.S. Citizenship and Immigration Services Employee and Co-Conspirator Arrested for Visa, Passport and Identification Fraud

We initiated an investigation after receiving allegations of immigration fraud and bribery by a USCIS employee. The investigation, which is being conducted jointly with the FBI, led to the June 29, 2006, arrest of the employee and a co-conspirator for violations of 18 USC § 1543 (*Passport Fraud*); 18 USC § 1028 *(Identification Fraud)*; and, 18 USC § 1546 (*Visa Fraud*). The employee and co-conspirator are currently being held without bond.

Former CIS Supervisor Accused of Harboring Aliens a Second Time

We conducted an investigation of a former USCIS supervisor, previously convicted of harboring aliens, who was found to be again harboring the same illegal alien after the alien was deported and re-entered the United States illegally. This investigation resulted in new indictments of the former USCIS supervisor and the illegal alien. The former supervisor was indicted and arrested on charges of 8 USC §1324, *Bringing in and Harboring Certain Aliens.* The former supervisor's probation for his previous conviction of 8 USC § 1324 (*Conspiracy to Smuggle Aliens*) was revoked. The former supervisor is currently incarcerated pending trial on the new charges. The illegal alien was indicted for 8 USC § 1326, *Re-Entry After Deportation.* The alien is currently a fugitive from justice.

USCIS District Adjudications Officer Accused of Sex Demand

A former USCIS district adjudications officer faces charges of attempted oral copulation and sexual battery under the color of authority of the state penal code. He was arrested and accused of ordering a Vietnamese woman to have sex with him in exchange for

approving her U.S. citizenship application. He will be tried on two felonies, "*Attempted Oral Copulation*," and "*Sexual Battery Under Duress*," violations of a state penal code. Trial is pending.

District Adjudication Officer and Sister Sell Green Cards

A suspicious activity report filed by a bank led to the arrest of a retired USCIS, district adjudication officer in Florida pursuant to a 13-count indictment. That indictment charged the officer, his sister, and 28 other defendants with conspiracy to fraudulently provide permanent resident documents or "green cards" to illegal aliens and money laundering. From April 2001 to November 2005, these conspirators allegedly provided hundreds of fraudulent green cards and received more than $1 million in proceeds. A single early morning joint operation led by ICE, our office and the FBI resulted in the arrests of 29 of the 30 defendants in Florida, New York, and North Carolina. The remaining defendant subsequently surrendered in New York. All defendants are pending judicial action.

Supervisory District Adjudication Officer Indicted For Falsifying Forms

A confidential informant of the FBI identified an alien resident who had allegedly been the beneficiary of immigration documents fraudulently approved by an unidentified immigration official. Our examination of the audit trail of the alien file for that alien identified a USCIS supervisory district adjudication officer as the official who had fraudulently approved that applicant for receipt of permanent resident status. Continued investigation by this office identified two other alien files which this officer had also inappropriately requested be transferred to his office from other districts. The officer subsequently forged a subordinate's signature and stamp to approve these files for receipt of permanent resident status. The officer was charged with falsifying documents and admitted to the offenses and was arrested on a two-count indictment, which continues pending judicial action.

UNITED STATES COAST GUARD

Annual Review of Mission Performance United States Coast Guard (FY 2005)

The *Homeland Security Act of 2002* requires that we annually assess the USCG's performance of all its missions. To address the Act's requirements, we reviewed the USCG's resource hours used to perform the various homeland security and non-homeland security missions, as well as performance goals and results, from FY 2001 through FY 2005. USCG data shows that total mission hours have increased in every period from FY 2001 through FY 2005, and since FY 2001 more resource hours have

been dedicated to homeland security missions than for non-homeland security missions. However, after an initial drop in FY 2002, non-homeland security resource hours have increased every period, and have now returned to within 3 percent of baseline levels. The USCG has been more successful in meeting goals for its traditional non-homeland security missions, meeting 22 of 28 goals (79 percent) where measurable goals and results existed, but still leaving room for improved performance. Not including the ports, waterways, and coastal security mission, by far the largest users of resource hours of any USCG mission, the USCG achieved only 26 percent of its homeland security goals (5 of 19). Growth in total resource hours has leveled off, and since resource hours are based on the limited and finite number of available assets, the USCG will be unable to increase total resource hours without the acquisition of additional aircraft, cutters, and boats. Consequently, the USCG has a limited ability to respond to an extended crisis, and therefore must divert resources normally dedicated to other missions. To improve performance within their overall constraints, the USCG must ensure that a comprehensive and fully defined performance management system is implemented, and that experienced and trained personnel are available to satisfy increased workload demands. (OIG-06-50, July 2006, OA)

Improvements Needed in the U. S. Coast Guard's Acquisition and Implementation of Deepwater Information Technology Systems

Declining readiness of "Deepwater" assets, including aircraft and cutters of various sizes, has hindered the USCG's effectiveness in accomplishing its homeland security, law enforcement, and regulatory missions. To meet the demand for improved communications, interoperability, and maritime security in today's environment, the USCG has embarked on an estimated 20-year, $20 billion acquisition to modernize and strengthen its aging Deepwater fleet.

We audited the USCG's efforts to design and implement command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems to support the Integrated Deepwater System program. As a result of our audit, we determined that the USCG's efforts to develop its Deepwater C4ISR systems could be improved. Although USCG officials are involved in high-level Deepwater IT requirements definition processes, they have limited influence over contractor decisions toward meeting these requirements. A lack of discipline in required change management processes provides little assurance that the requirements remain up-to-date or effective in meeting program goals. Certification and accreditation of Deepwater C4ISR equipment has been difficult to achieve, placing systems security and operations at risk. Further, although the Deepwater program has established IT testing procedures, the contractor has not followed them consistently to ensure that C4ISR systems and the assets on which they are installed perform effectively.

Additionally, the USCG faces several challenges to implementing effectively its Deepwater C4ISR systems. Due to limited oversight as well as unclear contract requirements, the agency cannot ensure that the contractor is making the best decisions toward accomplishing Deepwater IT goals. Insufficient C4ISR funding has restricted accomplishing the "system-of-systems" objectives that are considered fundamental to Deepwater asset interoperability. Inadequate training and guidance hinder users from realizing the full potential of the C4ISR upgrades. Instituting effective mechanisms for maintaining C4ISR equipment have been equally challenging.

To ensure success of the Deepwater program, we recommended that the commandant direct the program executive officer to address the C4ISR planning and implementation issues. Specifically, we recommended greater USCG involvement in requirements definition and change management processes as well as adherence to systems security assurance and testing procedures. Overcoming contractor oversight, systems integration, training, and IT support issues will be just as key. The USCG concurred with our recommendations and is in the process of implementing corrective measures. (OIG-06-55, August 2006, IT)

UNITED STATES SECRET SERVICE

USSS Contract Employee identified in the Theft of Computers at DHS HQ

We initiated an investigation after the DHS Office of Security reported that an USSS contract employee had been identified removing laptop computers from a warehouse at the DHS Headquarters building, Washington, DC. During an interview with us, the contract employee admitted to stealing approximately 60 computers and providing them to another USSS contract employee. Further investigation led to the recovery of one of the stolen items. The U.S. Attorney's Office for the District of Columbia accepted this case for prosecution. **Update:** On September 7, 2006, the subject was arrested on a warrant issued by a federal court for a violation of 18 USC § 641 (*Theft of Government Property*).

US-VISIT

Enhanced Security Controls Needed for US-VISIT's System Using RFID Technology

We audited DHS and select organizational components' security programs to evaluate the effectiveness of controls implemented on RFID systems. Our objective was to determine whether the US-VISIT program has implemented effective controls to protect critical data processed by its RFID system from unauthorized access. We interviewed

US-VISIT's technical staff; reviewed applicable DHS and US-VISIT policies and procedures; conducted vulnerability assessments of the databases and servers that collect and process information; and evaluated the effectiveness of physical security and assessed the security controls over the RFID-enabled Form I-94s and readers at selected POEs.

Overall, information security controls have been implemented to provide an effective level of security on the automated identification management system. US-VISIT has implemented effective physical security controls over the RFID tags, readers, computer equipment, and the database supporting the RFID system at the POEs visited. No personal information is stored on the tags used for US-VISIT. Travelers' personal information is maintained in and can be obtained only with access to the system's database. Additional security controls would need to be implemented if US-VISIT decides to store travelers' personal information on RFID-enabled forms or migrates to universally readable Generation 2 products.

Although these controls provide overall system security, US-VISIT has not properly configured its automated identification management system database to ensure that data captured and stored is properly protected. Furthermore, while its automated identification management system is operating with an authority to operate, US-VISIT had not tested its contingency plan to ensure that critical operations could be restored in the event of a disruption. In addition, US-VISIT has not developed its own RFID policy or ensured that the standard operating procedures are properly distributed and followed at all POEs.

We recommended that US-VISIT: (1) develop and implement procedures to strengthen user account and password management processes relating to the automated identification management system database; (2) ensure that all vulnerabilities identified for which risks have not been assumed be remedied; (3) test contingency plans, at least annually; and, (4) develop and implement its own policy that addresses security controls over all components of an RFID system and ensures that policies and procedures are being followed at all affected POEs. US-VISIT agreed and has already taken steps to implement each of the recommendations. (OIG-06-39, June 2006, IT)

OTHER OIG ACTIVITIES

Oversight of Non-DHS OIG Audits

We processed 53 contract audits conducted by DCAA during the current reporting period. These reports contained $4,601,431 in questioned costs of which all were determined to be unsupported costs. In addition, DCAA identified $31,404 as "funds put

to better use" resulting from its review of a contractor's proposal. We continue to monitor the actions taken to implement the recommendations in the reports.

We also processed 52 single audit reports issued by other independent public accountant organizations. The single audit reports questioned $4,389,862 of which $3,222,431 was determined to be unsupported costs. The reports were conducted according to the *Single Audit Act of 1996*, as amended by PL 104-136. We continue to monitor the actions taken to implement the recommendations in the reports.

Significant Reports Unresolved Over Six Months

Timely resolution of outstanding audit recommendations continues to be a priority of both our office and the department. As of this report date, we are responsible for monitoring 216 reports that contain recommendations that have been unresolved for more than six months. Management decisions have not been made for significant reports, as follows:

- Twenty-three program management audit reports.

  The Department is currently reviewing the reports and advises that it anticipates resolving the recommendations by March 31, 2007.

- Fifty-three grant compliance audit reports.

  The Department is currently reviewing the reports and advises that it anticipates resolving the recommendations by March 31, 2007.

- Eleven state disaster management contract audit reports.

  The Department is currently reviewing the reports and advises that it anticipates resolving the recommendations by March 31, 2007.

- Seventy-three Single Audit Act reports.

  The Department is currently reviewing the reports and advises that it anticipates resolving the recommendations by March 31, 2007.

- Seventeen DCAA contract audit reports.

  The Department is currently reviewing the reports and advises that it anticipates resolving the recommendations by March 31, 2007.

- Nine audit reports issued by legacy agencies other than FEMA.

  The Department is currently reviewing the reports and advises that it anticipates resolving the recommendations by March 31, 2007.

LEGISLATIVE AND REGULATORY REVIEW

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

During this reporting period, we reviewed 68 legislative and regulatory proposals, draft DHS policy directives, and other items. The topics concerned diverse subjects including HR 3041, the "*Privacy Officer with Enhanced Rights Act of 2005*," draft legislation establishing the Disaster Assistance Fraud Prevention Program, proposed restructuring of FEMA, and terrorist information sharing. Some of these items are highlighted below.

Draft DHS Policy on Corrective Action Plans: We commented on a draft directive establishing DHS policy for developing, maintaining, reporting, and monitoring corrective action plans to support compliance with the *Federal Managers' Financial Integrity Act* and Office of Management and Budget guidance. We emphasized the need to provide more substantive guidance on corrective action plans, and made several recommendations for clarifying key roles and responsibilities. DHS management adopted our recommended changes.

Proposed Whistleblower Protection Amendment: We reviewed a legislative proposal to provide whistleblower protections for all employees serving in DHS, including the TSA. The proposal was modeled on the whistleblower protections afforded to private airline industry employees by Section 42121 of Title 49, U.S. Code. We suggested, among other things, that the proposal's intended purpose would be better served by extending existing whistleblower protections now applicable for most federal employees, rather than developing entirely new protections modeled on a private industry complaint procedure.

Draft DHS Directives on Gifts to Employees, and Gifts to the Department of Homeland Security: We commented on two draft DHS directives involving gifts. The first directive, *Gifts to Employees*, proposed policies and procedures for the acceptance, use and accountability of both foreign gifts and gifts to individuals. We recommended limiting the directive's scope to foreign gifts. We noted that gifts to individuals are governed by the Standards of Ethical Conduct for Employees of the Executive Branch, and that conflicting supplemental guidance cannot be issued without concurrence from the Office of Government Ethics. For the second directive, *Gifts to the Department of Homeland Security*, we recommended establishing a monetary threshold for gifts to DHS that must be reviewed by the DHS gifts committee to allow components to determine whether to accept gifts with minimal value.

Proposed Changes to Government Auditing Standards: We reviewed proposed revisions to the Government Auditing Standards, commonly known as the "Yellow Book." We provided numerous comments and recommendations regarding the clarity and consistency of information. For example, we noted that the discussion of non-audit services did not clearly indicate if this applied to the audit manager/supervisor only or to the auditor. We also recommended providing additional guidance and examples for several areas (e.g., how identified "abuse" impacts issuing financial statement opinions and making required disclosures, reporting requirements and level of support needed for identifying "potential fraud;" and independent public accounting firm documentation, including responsibilities and limitations on gaining access). Finally, in comparing the 2003 Yellow Book requirements with the proposed revision, we noted that the 2003 requirements more clearly defined a documenting system of quality control

Draft DHS Strategic Plan for 2006-2011: As an overall observation, we commented that without more mapping of operations to strategic goals, the draft document was more of a policy statement, not a strategic plan. We also noted that the draft Plan did not explain how states will share information with DHS, and that it made redundant use of various disaster-related terms.

CONGRESSIONAL BRIEFINGS AND TESTIMONY

Congressional Briefings and Testimony

Extensive dialogue with congressional members and their staff continued throughout the reporting period. Our office conducted numerous briefings for congressional staff on results of our work, including a review of Canadian waste shipments; individual state's management of first responder grant funds; Federal Protective Service funds transferred from the General Services Administration to DHS; actions taken by CBP to intercept

suspected terrorists at U.S. POEs; ICE-CBP issues; development of the national asset database; detention and removal of illegal aliens; and, security vulnerabilities of the transportation worker identification credential program. Meetings to discuss other congressional concerns included prescription drug seizures, USCG Deepwater program, FEMA reorganization, and corruption at our borders.

To ensure our stakeholders have an opportunity to participate in the development of our Annual Performance Plan for 2007, we sought and received input from DHS and from our congressional oversight committees. We met with congressional members and staff to discuss the final 2007 plan. The Annual Performance Plan is OIG's "roadmap" for the inspections and audits that it plans to conduct each year to evaluate the department's programs and operations.

The IG testified seven times before the following congressional committees on issues such as USCG's mission performance, financial management, information sharing, border security, federal assistance to New York following the terrorist attacks of September 11, 2001, and waste, fraud and abuse in the aftermath of Hurricane Katrina. OIG testimony may be accessed through our website at: www.dhs.gov/oig.

- September 14, 2006 - House Committee on Transportation and Infrastructure, Subcommittee on USCG and Maritime Transportation, on the USCG's mission performance for FY 2005 and to examine the USCG's efforts to balance its assets and personnel to carry out its various traditional and homeland security missions.

- September 13, 2006 - House Government Reform, Subcommittee on Government Management, Finance, and Accountability, on the department's ongoing efforts to improve agency financial management.

- September 13, 2006 - House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, an update on the department's information sharing efforts and the evolution of the department's Homeland Security Information Network.

- July 27, 2006 - House Committee on Government Reform, on the acquisition function of the department.

- July 20, 2006 – A Joint Hearing of the House Committee on Government Reform, Subcommittee on Criminal Justice, Drug Policy, and Human Resources, and the House Committee on Homeland Security, Subcommittee on Economic Security, Infrastructure Protection, and Cyber-Security, on fencing the southwest border including construction options and strategic placement.

- July 12, 2006 - House Committee on Homeland Security, Subcommittee on Management, Integration and Oversight, on federal assistance to New York following terrorist attacks on September 11, 2001, including lessons learned in fraud detection, prevention, and control.

- April 21, 2006 - Field Hearing, Senate Committee on Homeland Security and Governmental Affairs, "FEMA's Manufactured Housing Program: Haste Makes Waste," Hope, AR.

GULF COAST HURRICANE RECOVERY

- April 10, 2006 - Field Hearing, Senate Subcommittee on Federal Financial Management, Government Information and International Security, Committee on Homeland Security and Governmental Affairs, "Management and Oversight of Federal Disaster Recovery: Debris Removal, Blue Roof Program, Haul and Install Case Studies," New Orleans, LA.

- May 4, 2006 - House Committee on Government Reform, "Federal Contracting in Disaster Preparedness and Response,"

- May 10, 2006 - House Subcommittee on Government Management, Finance and Accountability, Committee on Government Reform, "After Katrina. The Role of the Department of Justice, Katrina Fraud Task Force and Agency Inspectors General in Preventing Waste, Fraud, and Abuse,"

***Congressional Delegation*:**

- April 24-26, 2006 - Rep. Todd R. Platts, (R-PA), Committee on Government Reform (Government Management, Finance & Accountability – Chairman). Gulf Coast tour, IG and Katrina Task Force briefings.

***Briefings*:**

- May 3, 2006 - Minority and Majority Staff Briefing, House Oversight and Investigations Subcommittee, Committee on Transportation & Infrastructure.

- May 4, 2006 - Minority and Majority Staff Briefing, House Oversight and Investigations Subcommittee, Committee on Energy and Commerce.

- May 18, 2006 - Majority Staff Briefing, House Survey and Investigations Subcommittee, Committee on Appropriations.

- June 26, 2006 - Minority and Majority staff, House Homeland Security. Topic: Inspection report.

- June 27, 2006 – Minority and Majority House Survey and Investigations Subcommittee, Committee on Appropriations.

- August 15, 2006 - House HSGAC, staff counsel briefing, Cherri Branson Topic: Prompt-payment issues.

- August 28, 2006 - Majority Staff, House Subcommittee on Homeland Security, Appropriations Committee

APPENDICES

Appendix 1
Audit Reports With Questioned Costs

Report Category	Number	Questioned Costs	Unsupported Costs
A. Reports pending management decision at the start of the reporting period[1]	116	$167,896,996	$63,131,775
B. Reports issued/processed during the reporting period with questioned costs	30	$46,365,569	$13,786,763
Total Reports (A+B)	146	$214,262,565	$76,918,538
C. Reports for which a management decision was made during the reporting period	7	$2,926,356	$ 822,106
(1) Disallowed costs	1	$1,592	$0
(2) Accepted costs	6	$2,924,764	$822,106
D. Reports put into appeal status during period	0	$0	$0
E. Reports pending a management decision at the end of the reporting period	139	$211,336,209	$76,096,432
F. Reports for which no management decision was made within six months of issuance	109	$164,970,640	$62,309,669

Notes and Explanations:

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

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

[1] One single audit report (OIG-S-41-06) was inadvertently processed as a duplicate during the previous semiannual reporting period ending March 2006. As a result, the beginning balances in Section A above were amended to account for the error. We reduced the number of reports in the beginning balance by 1. We also reduced both the questioned costs and unsupported costs by $447,737, respectively.

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

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

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

Appendix 1b
Audit Reports With Funds Put to Better Use

Report Category	Number	Amount
A. Reports pending management decision at the start of the reporting period	12	$122,678,958
B. Reports issued during this reporting period	2	$73,531,404
Total Reports (A + B)	14	$196,210,362
C. Reports for which a management decision was made during the reporting period	3	$132,746,690
(1) Value of recommendations agreed to by management	3	$132,746,690
(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	11	$63,463,672
F. Reports for which no management decision was made within six months of issuance	10	$63,432,268

Notes and Explanations:

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

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

Appendix 2
Compliance – Resolution of Reports and Recommendations

MANAGEMENT DECISION IS PENDING

3/31/06	
Reports open over six months	201
Recommendations open over six months	791
9/30/2005	
Reports open over six months	216
Recommendations open over six months	989

CURRENT INVENTORY

Open reports at the beginning of the period[1]	430
Reports issued this period[2]	178
Reports closed this period	204
Open reports at the end of the period	404

ACTIVE RECOMMENDATIONS

Open recommendations at the beginning of the period[1]	1,393
Recommendations issued this period	426
Recommendations closed this period	131
Open recommendations at the end of the period	1,688

Notes and Explanations:

[1] The beginning balances for "Current Inventory" and "Active Recommendations" were amended to compensate for a report that was processed in error in the prior Semiannual Report to Congress.
[2] Includes 11 management audit reports issued, 16 IT audit reports issued, 5 inspection reports issued, 29 management advisory reports, 1 Gulf Coast management report, 11 disaster grant audit reports issued, 53 DCAA audit reports processed, and 52 single audit reports processed.

Appendix 3
Management Reports Issued

	Program Office/Report Subject	Report Number	Date Issued
1.	Detention and Removal of Illegal Aliens, U.S. Immigration and Customs Enforcement (ICE)	OIG-06-33	4/06
2.	Review of the Transportation Security Administration (TSA) Collection of Aviation Security Service Fees	OIG-06-35	5/06
3.	CBP's Trusted Traveler Systems Using RFID Technology Require Enhanced Security	OIG-06-36	5/06
4.	Buy American Act Compliance	OIG-06-37	5/06
5.	Homeland Security Information Network Could Support Information Sharing More Effectively	OIG-06-38	6/06
6.	Enhanced Security Controls Needed for US-VISIT's System Using RFID Technology	OIG-06-39	6/06
7.	Progress in Developing the National Asset Database	OIG-06-40	6/06
8.	Information Technology Management Letter for the FY 2005 Customs and Border Protection Balance Sheet Audit	OIG-06-41	6/06
9.	Improved Administration Can Enhance Science and Technology Laptop Computer Security	OIG-06-42	6/06

Appendix 3
Management Reports Issued

	Program Office/Report Subject	Report Number	Date Issued
10.	Review of CBP Actions Taken to Intercept Suspected Terrorists at U.S. Ports of Entry	OIG-06-43	6/06
11.	TSA's Development of Its Weapons Management System Using RFID	OIG-06-44	7/06
12.	DHS' Management of Automated Procurement Systems Needs Improvement	OIG-06-46	7/06
13.	DHS Must Address Significant Security Vulnerabilities Prior To TWIC Implementation	OIG-06-47	7/06
14.	Special Report: Letter on TSA's FY 2005 Financial Statements	OIG-06-48	7/06
15.	Information Technology Management Letter for the FY 2005 DHS Financial Statement Audit	OIG-06-49	7/06
16.	Annual Review of Mission Performance United States Coast Guard (FY 2005)	OIG-06-50	7/06
17.	Management Letter for the FY 2005 DHS Financial Statement Audit	OIG-06-51	7/06
18.	Audit of DHS' Corrective Action Plan Process for Financial Reporting – Report No. 1	OIG-06-52	7/06

Appendix 3
Management Reports Issued

	Program Office/Report Subject	Report Number	Date Issued
19.	Additional Guidance and Security Controls Are Needed Over Systems Using RFID at DHS	OIG-06-53	7/06
20.	Audit of the National Urban Search and Rescue Response System	OIG-06-54	8/06
21.	Improvements Needed in the U. S. Coast Guard's Acquisition and Implementation of Deepwater Information Technology Systems	OIG-06-55	8/06
22.	Survey of DHS Data Mining Activities	OIG-06-56	8/06
23.	A Review of Immigration and Customs Enforcement Discipline Procedures	OIG-06-57	8/06
24.	Office of Inspector General Laptop Computers Are Susceptible To Compromise	OIG-06-58	8/06
25.	Evaluation of DHS' Security Program and Practices For Its Intelligence Systems For Fiscal Year 2006	OIG-06-59	8/06
26.	Transportation Security Administration Continuity of Operations Program	OIG-06-60	8/06
27.	Audit of DHS' Corrective Action Plan Process for Financial Reporting – Report No. 2	OIG-06-61	9/06

Appendix 3
Management Reports Issued

	Program Office/Report Subject	Report Number	Date Issued
28.	Evaluation of DHS' Information Security Program for Fiscal Year 2006	OIG-06-62	9/06
29.	Improved Administration Can Enhance Science and Technology Classified Laptop Computer Security	OIG-06-63	9/06
30.	Improved Administration Can Enhance U.S. Customs and Border Protection Classified Laptop Computer Security	OIG-06-64	9/06
31.	Review of TSA Non-Screener Administrative Positions	OIG-06-65	9/06
32.	Audit of Payments to the Automated Commercial Environment (ACE) Contractors	OIG-06-66	9/06
33.	Purchase Cards: Control Weaknesses Leave DHS Highly Vulnerable to Fraudulent, Improper, and Abusive Activity	GAO-06-1117	9/06

Appendix 4
Financial Assistance Audit Reports Issued

	Report Number	Date Issued	Auditee	Questioned Costs	Unsupported Costs	Funds Put to Better Use
1.	GC-FL-06-30	4/06	Review of Hurricane Wilma Activities Solid Waste Authority of Palm Beach County, Florida FEMA Disaster No. 1609-DR-FL	$0	$0	$0
2.	GC-AL-06-31	4/06	Black Warrior Electric Membership Cooperative - FEMA Disaster 1605-DR-AL	$2,242	$0	$0
3.	GC-TX-06-32	4/06	Review of Hurricane Katrina Activities City of Austin, Texas FEMA Disaster Number EM-3216-TX	$0	$0	$0
4.	GC-FL-06-33	4/06	Review of Hurricane Wilma Activities Miami-Dade County, FLorida FEMA Disaster 1609-DR-FL	$0	$0	$73,500,000
5.	GC-HQ-06-34	4/06	Reimbursement for Other Needs Assistance Items	$0	$0	$0
6.	GC-HQ-06-35	4/06	Cannibalization of Travel Trailers by Bechtel	$0	$0	$0
7.	GC-MS-06-36	4/06	Review of Hurricane Katrina Activities City of Wiggins, Mississippi FEMA Disaster Number 1604-DR-MS	$0	$0	$0
8.	GC-MS-06-37	4/06	Review of Hurricane Katrina Activities Dixie Electric Power Association FEMA Disaster No 1604-DR-MS	$207,068	$0	$0

Appendix 4
Financial Assistance Audit Reports Issued

	Report Number	Date Issued	Auditee	Questioned Costs	Unsupported Costs	Funds Put to Better Use
9.	GC-AL-06-38	4/06	Review of Hurricane Katrina Activities City of Tuscaloosa, AL	$0	$0	$0
10.	GC-FL-06-39	4/06	Review of Hurricane Wilma Activities Collier County, Florida FEMA Disaster No. 1609-DR-FL	$0	$0	$0
11.	GC-HQ-06-40	4/06	Review of FEMA Policy for Funding Public Assistance Administrative Costs	$0	$0	$0
12.	GC-HQ-06-41	6/06	Management Advisory Report on Contract HSFEHQ-06-C-0024 to Provide Assistance to Eligible Evacuees in Need of Housing and Pharmaceuticals	$0	$0	$0
13.	GC-FL-06-42	4/06	Review of Hurricane Wilma Activities, St. Lucie County, Florida FEMA Disaster No. 1609-DR-FL	$0	$0	$0
14.	GC-TX-06-43	6/16	Review of Hurricane Katrina Activities Dallas Housing Authority, Dallas, Texas FEMA Disaster Number EM-3216-TX	$0	$0	$0
15.	GC-FL-06-44	6/16	Review of Hurricane Wilma Activities City of Plantation, Florida - FEMA Disaster No. 1609-DR-FL	$0	$0	$0
16.	GC-HQ-06-45	7/06	Improvements Needed in the Classification and Distribution of Hurricane Katrina Disaster Relief Costs	$0	$0	$0

Appendix 4
Financial Assistance Audit Reports Issued

	Report Number	Date Issued	Auditee	Questioned Costs	Unsupported Costs	Funds Put to Better Use
17.	GC-FL-06-46	7/06	Review of FEMA Contracts Awarded by Contracting Officers at the Orlando, Florida Long Term Recovery Office	$0	$0	$0
18.	GC-MS-06-47	8/06	Review of Hurricane Katrina Activities Pearl River County, Mississippi, FEMA Disaster Number 1604-DR-MS	$0	$0	$0
19.	GC-MS-06-48	8/06	Review of Hurricane Katrina Activities Stone County, Mississippi FEMA Disaster No. 1604-DR-MS	$0	$0	$0
20.	GC-MS-06-49	8/06	Review of Hurricane Katrina Activities Magnolia Electric Power Association FEMA Disaster No 1604-DR-MS	$88,933	$0	$0
21.	GC-FL-06-50	8/06	Review of Hurricane Wilma Activities, City of Fort Lauderdale, Florida FEMA Disaster Number 1609-DR-Fl	$0	$0	$0
22.	GC-HQ-06-51	8/06	Debit Card Overdrafts	$0	$0	0
23.	GC-HQ-06-52	9/06	Management Advisory Report on the Starship Facility Renovation Project, Anniston, Alabama	$0	$0	$0

Appendix 4
Financial Assistance Audit Reports Issued

	Report Number	Date Issued	Auditee	Questioned Costs	Unsupported Costs	Funds Put to Better Use
24.	GC-HQ-06-53	9/06	Review of Hurricane Katrina Activities FEMA Disaster No. 1603-DR-LA City of New Orleans, Louisiana Appeal Process for Residential Damage Assessments	$0	$0	$0
25.	GC-LA-06-54	9/06	Interim Review of Hurricane Katrina Activities, St. Bernard Parish, Louisiana - FEMA Disaster No. 1603-DR-LA Public Assistance Identification Number 087-99087-00	$0	$0	$0
26.	GC-MS-06-55	9/06	Review Hurricane Katrina Activities City of Long Beach, Mississippi FEMA Disaster Number 1604-DR-MS	$12,850	$0	$0
27.	GC-LA-06-56	9/06	Interim Review of Hurricane Katrina Activities, City of New Orleans, Louisiana FEMA Disaster No. 1603-DR-LA Public Assistance Identification Number 071-55000-00	$0	$0	$0
28.	GC-LA-06-57	9/06	Review of Hurricane Activities Congressional Inquiry, Contingency Payment of Contractors in St. Tammany Parish, Louisiana	$0	$0	$0

Appendix 4
Financial Assistance Audit Reports Issued

	Report Number	Date Issued	Auditee	Questioned Costs	Unsupported Costs	Funds Put to Better Use
29.	GC-TX-06-58	9/06	Review of Hurricane Katrina Activities, City of Houston, Texas FEMA Disaster Number EM-3216-TX	$0	$0	$0
			Subtotal: Gulf Coast Hurricane Recovery Related Reports	**$311,093**	**$0**	**$73,500,000**
30.	DD-08-06	6/06	University of North Dakota, Grand Forks, North Dakota	$2,254,367	$0	$0
31.	DD-09-06	7/06	City of Kansas City, Missouri	$6,976,274	$4,446,217	$0
32.	DD-10-06	8/06	Grand Forks Public School District, Grand Forks, North Dakota	$24,656,533	$186,899	$0
33.	DD-11-06	9/06	Recap of Procurement Problems Identified in Audits of Electric Cooperatives	$0	$0	$0
34.	DS-02-06	4/06	Audit of San Francisco Unified School District, San Francisco, California	$464,284	$458,076	$0
35.	DS-03-06	4/06	Audit of Sonoma County, Santa Rosa California	$331,983	$251,012	$0

Appendix 4
Financial Assistance Audit Reports Issued

	Report Number	Date Issued	Auditee	Questioned Costs	Unsupported Costs	Funds Put to Better Use
36.	DS-04-06	4/06	Audit of State of Washington's Department of Corrections, Olympia, Washington	$1,592	$0	$0
37.	DS-05-06	7/06	Audit of Los Angeles County Department of Public Works, Alhambra, California	$1,632,109	$0	$0
38.	DS-06-06	8/06	Audit of the County of Contra Costa, Martinez, California	$33,756	$14,543	$0
40.	OIG-06-34	5/06	Audit of Grant 2004-TK-TX-003 and 2005-GH-T5-0001 Awarded to the National Domestic Preparedness Coalition of Orlando, Florida	$240,517	$134,386	$0
41.	OIG-06-45	7/06	The Commonwealth of Virginia's Management of State Homeland Security Grants Awarded During Fiscal Years 2002 and 2003	$471,768	$471,768	$0
			Subtotal Grant Audits	$37,063,183	$5,962,901	$0
42.	OIG-C-87-06	6/06	Report on Audit of Northern Material Acquisition Center Allocations	$2,081,500	$2,081,500	$0

Appendix 4
Financial Assistance Audit Reports Issued

	Report Number	Date Issued	Auditee	Questioned Costs	Unsupported Costs	Funds Put to Better Use
43.	OIG-C-96-06	8/06	Audit of Proposal for Time and Material Delivery Order L-3 Communications, Security and Detection System	$0	$0	$31,404
44.	OIG-C-112-06	9/06	Report on Invoice Verification: TeleTech Government Solutions	$2,518,124	$2,518,124	$0
45.	OIG-C-119-06	9/06	Evaluation of ISO CY 2005 Billed Costs – Insurance Services Office (ISO)	$1,807	$1,807	$0
			Subtotal DCAA Audits[1]	**$4,601,431**	**$4,601,431**	**$31,404**
46.	OIG-S-61-06	4/06	City of Escondido, California	$262,356	$0	$0
47.	OIG-S-65-06	5/06	City of Miami, Florida	$272,267	$0	$0
48.	OIG-S-67-06	5/06	City of Murfreesboro, Tennessee	$2,601	$2,601	$0
49.	OIG-S-71-06	5/06	City of Phoenix, Arizona	$192,855	$0	$0
50.	OIG-S-76-06	6/06	State of Delaware	$613,707	$613,707	$0
51.	OIG-S-77-06	06/06	Commonwealth of Kentucky	$98,679	$98,679	$0

[1] Includes only those DCAA audit reports that disclosed questioned costs. All DCAA audit reports processed are included in the Statistical Highlights.

Appendix 4
Financial Assistance Audit Reports Issued

	Report Number	Date Issued	Auditee	Questioned Costs	Unsupported Costs	Funds Put to Better Use
52.	OIG-S-78-06	06/06	State of Florida	$45,791	$0	$0
53.	OIG-S-82-06	07/06	State of Nebraska	$ 1,489,257	$ 1,489,257	$0
54.	OIG-S-83-06	07/06	State of New Hampshire	$63,513	$63,513	$0
55.	OIG-S-85-06	08/06	State of North Carolina	$757,370	$757,370	$0
56.	OIG-S-95-06	08/06	State of Washington	$150,000	$150,000	$0
57.	OIG-S-108-06	9/06	Cleveland-Cuyahoga County Port Authority	$394,162	$0	$0
58.	OIG-S-110-06	9/06	County of San Saba, Texas	$47,304	$47,304	$0
			Subtotal Single Audits[1]	**$4,389,862**	**$3,222,431**	**$0**
			Grand Total Financial Assistance	**$46,365,569**	**$13,786,763**	**$73,531,404**

Note: The narrative identifies 100 percent of the dollar amount we questioned. This appendix reflects the actual breakdown of what the grantee is expected to de-obligate or reimburse – there is a percentage of what they pay vs. what we pay that we calculate.

Report Number Acronyms:
DD Disaster, Denton/Dallas Office
DS Disaster, San Francisco/Oakland Office

[1] Includes Single Audit reports that disclosed questioned costs. All single audit reports processed are included in the Statistical Highlights.

Appendix 5
Schedule of Amounts Due and Recovered

	Report Number	Date Issued	Auditee	Amount Due	Recovered Costs
1.	DS-04-06	04/06	Audit of State of Washington's Department of Corrections, Olympia, Washington	$0	$1,592
2.	H-S-35-01	5/01	Government of the U.S. Virgin Islands	$0	$2,158,488
			TOTAL	**$0**	**$2,160,080**

Report Number Acronyms:

DS Disaster, San Francisco
H-S Single Audits

Appendix 6
Acronyms

CBP	Customs and Border Protection
COOP	Continuity of Operations Plan
DCAA	Defense Contract Audit Agency
DD	Disaster, Dallas
DHS	Department of Homeland Security
DS	Disaster, San Francisco
FAM	Federal Air Marshal
FBI	Federal Bureau of Investigations
FEMA	Federal Emergency Management Agency
FY	Fiscal Year
GAO	Government Accountability Office
GC	Gulf Coast Hurricane Recovery Office
HSIN	Homeland Security Information Network
ICE	Immigration and Customs Enforcement
IG	Inspector General
ISP	Office of Inspections
IT	Information Technology
OA	Office of Audits
OIG	Office of Inspector General
OIG-C	DCAA Audits
OIG-S	Single Audits
POE	Ports of Entry
PL	Public Law
RFID	Radio Frequency Identification
S&T	Science & Technology
TSA	Transportation Security Administration
USC	United States Code
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Services
US-VISIT	U.S. Visitor and Immigrant Status Indicator Technology
USSS	United States Secret Service

Appendix 7
OIG Headquarters/Field Office Contacts and Locations

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

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

OIG Headquarters Senior Management Team

Richard L. Skinner	.....	**Inspector General**
James L. Taylor	.....	**Deputy Inspector General**
Richard N. Reback	.....	**Counsel to the Inspector General**
David M. Zavada	.....	**Assistant Inspector General/Audits**
Elizabeth M. Redman	.....	**Assistant Inspector General/Investigations**
Carlton I. Mann	.....	**Acting Assistant Inspector General/ Inspections**
Frank Deffer	.....	**Assistant Inspector General/Information Technology**
Edward F. Cincinnati	.....	**Assistant Inspector General/Administration**
Matt Jadacki	.....	**Special Inspector General/Gulf Coast Hurricane Recovery**
Tamara Faulkner	.....	**Congressional Liaison and Media Affairs**
Denise S. Johnson	.....	**Executive Assistant to the Inspector General**

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

Atlanta, GA
10 Tenth St., NE., Suite 750
Atlanta, GA 30309
(404) 832-6700 / Fax (404) 832-6645

Boston, MA
10 Causeway Street, Suite 465
Boston, MA 02222
(617) 223-8600 / Fax (617) 223-8651

Chicago, IL
55 W. Monroe St., Suite 1010
Chicago, IL 60603
(312) 886-6300 / Fax (312) 886-6308

Dallas, TX
3900 Karina St., Suite 224
Denton, TX 76208
(940) 891-8900 / Fax (940) 891-8948

Houston, TX
5850 San Felipe Rd., Suite 300
Houston, TX 77057
(713) 706-4611 / Fax (713) 706-4625

Indianapolis, IN
5915 Lakeside Blvd.
Indianapolis, IN 46278
(317) 298-1596 / Fax (317) 298-1597

Kansas City, MO
901 Locust, Suite 470
Kansas City, MO 64106
(816) 329-3880 / Fax (816) 329-3888

Los Angeles, CA
222 N. Sepulveda Blvd., Suite 1680
El Segundo, CA 90245
(310) 665-7300 / Fax (310) 665-7302

Miami, FL
3401 SW 160th Ave., Suite 320
Miramar, FL 33027
(954) 538-7842 / Fax (954) 602-1034

Oakland, CA
300 Frank H. Ogawa Plaza, Suite 275
Oakland, CA 94612
(510) 637-1482 / Fax (510) 637-1484

Philadelphia, PA
Greentree Executive Campus
5002 D Lincoln Drive West
Marlton, NJ 08053-1521
(856) 968-4907 / Fax (856) 968-4914

St. Thomas, VI
5500 Veteran's Drive
Federal Bldg., Room 207
St. Thomas, VI 00802
(340) 774-0190 / Fax (340) 774-0191

San Juan, PR
654 Munoz Rivera Ave., Suite 1700
San Juan, PR 00918
(787) 294-2500 / Fax (787) 771-3620

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

Atlanta, GA
The Millennium in Midtown
10 Tenth St., NE, Suite 750
Atlanta, GA 30309
(404) 832-6730 / Fax (404) 832-6646

Baton Rouge, LA
Louisiana State University
402 Johnston Hall (Attn: DHS OIG-Inv)
Baton Rouge, LA 70803
(225) 334-4900 / Fax: (225) 334-4707

Biloxi, MS
FEMA/JFO
2350 Beach Blvd. (Attn: OIG Inv)
Biloxi, MS 39531
(228) 385-4933 / Fax: (228) 385-7148

Boston, MA
10 Causeway Street, Suite 465
Boston, MA 02222
(617) 565-8705 / Fax (617) 565-8995

Buffalo, NY
130 S. Elmwood Ave., Room 501
Buffalo, NY 14202
(716) 551-4231 / Fax (716) 551-4238

Chicago, IL
55 W. Monroe St., Suite 1050
Chicago, IL 60603
(312) 886-2800 / Fax (312) 886-2804

Dallas, TX
3900 Karina St., Suite 228
Denton, TX 76208
(940) 891-8930 / Fax (940) 891-8959

Del Rio, TX
Amistad National Recreation Area
4121 Highway 90 West
Del Rio, TX 78840
(830) 775-7492 x239

Detroit, MI
Fordland
4121 Town Center Dr., Suite 604
Detroit, MI 48126
(313) 226-2163 / Fax (313) 226-6405

El Centro, CA
516 Industry Way, Suite B
Imperial, CA 92251
(760) 335-3900 / Fax (760) 335-3726

El Paso, TX
1200 Golden Key Circle, Suite 230
El Paso, TX 79925
(915) 629-1800 / Fax (915) 594-1330

Hattiesburg, MS
6068 US Hwy 98 W, Suite 1258
Hattiesburg, MS 39402-8881
(601) 264-8220 / Fax: (601) 264-9088

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

Houston, TX
5850 San Felipe Rd., Suite 300
Houston, TX 77057
(713) 706-4600 / Fax (713) 706-4622

Laredo, TX
901 Victoria St., Suite G
Laredo, TX 78045
(956) 796-2917 / Fax (956) 717-0395

Los Angeles, CA
222 N. Sepulveda Blvd., Suite 1640
El Segundo, CA 90245
(310) 665-7320 / Fax (310) 665-7309

McAllen, TX
Bentsen Tower
1701 W. Business Highway 83, Suite 250
McAllen, TX 78501
(956) 664-8010 / Fax (956) 618-8151

Miami, FL
3401 SW 160th Ave., Suite 401
Miramar, FL 33027
(954) 538-7555 / Fax (954) 602-1033

Mobile, AL
DHS-OIG Alabama JFO
1141 Montlimar Dr., Suite 2500
Mobile, AL 36609
(251) 344-1487 / Fax: (251) 343-9779

New York City, NY
111 Pavonia Ave., Suite 630
Jersey City, NJ 07310
(201) 356-1800 / Fax (201) 356-4038

Oakland, CA
300 Frank H. Ogawa Plaza, Suite 275
Oakland, CA 94612
(510) 637-4311 / Fax (510) 637-4327

Orlando, FL
FEMA Long Term Recovery Office
100 Sunport Lane
Attn.: SA James DePalma
Orlando, FL 32809-7892

Philadelphia, PA
Greentree Executive Campus
5002 B Lincoln Drive West
Marlton, NJ 08053
(856) 596-3800 / Fax (856) 810-3410

San Diego, CA
701 B St., Suite 560
San Diego, CA 92101
(619) 557-5970 / Fax: (619) 557-6518

San Juan, PR
654 Plaza
654 Munoz Rivera Ave., Suite 1700
San Juan, PR 00918
(787) 294-2500 / Fax (787) 771-3620

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

Seattle, WA
2350 Carillon Point
Suite 2360
Kirkland, WA 98033
(425) 250-1260 / Fax (425) 576-0898

St. Thomas, VI
Office 550 Veterans Dr., Suite 207A
St. Thomas, VI 00802
(340) 777-1792 / Fax (340) 777-1803

Tucson, AZ
2120 West Ina Rd., Suite 201
Tucson, AZ 85741
(520) 229-6421 / Fax (520) 742-7192

Washington, DC
(Washington Field Office)
1300 North 17th St., Suite 510
Arlington, VA 22209
(703) 235-0848 / Fax (703) 235-0854

Yuma, AZ
775 E. 39th St., Room 216
Yuma, AZ 85365
(928) 314-9640 / Fax (928) 314-9640

Appendix 7
OIG Headquarters/Field Office Contacts and Locations
Locations of Gulf Coast Hurricane Recovery Field Offices

Biloxi, MS
2350 Beach Blvd. (Attn: DHS-OIG)
Biloxi, MS 39531
(228) 385-5605 / Fax: (228) 385-7149
(*Jointly occupied with Office of Investigations*)

Jackson, MS
FEMA JFO
515 Amite Street
Jackson, MS 39201
(601) 965-2599 / Fax (601) 965-2432

New Orleans, LA
One Seine Court, Room 516
New Orleans, LA 70114
(504) 762-2151 / Fax (504) 762-2873

Orlando, FL
FEMA Long Term Recovery Office
100 Sunport Lane
Orlando, FL 32809-7892
(407) 856-3204

Investigative Gulf Coast Hurricane Recovery Field Offices

Baton Rouge, LA
Louisiana State University
402 Johnston Hall (Attn: DHS OIG-Inv)
Baton Rouge, LA 70803
(225) 334-4900 / Fax: (225) 334-4707

Hattiesburg, MS
6068 US Hwy 98 W, Suite 1258
Hattiesburg, MS 39402-8881
(601) 264-8220 / Fax: (601) 264-9088

Mobile, AL
DHS-OIG Alabama JFO
1141 Montlimar Dr., Suite 2500
Mobile, AL 36609
(251) 344-1487 / Fax: (251) 343-9779

Appendix 8
Index to Reporting Requirements

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

Requirement:	**Pages**
Review of Legislation and Regulations	66-67
Significant Problems, Abuses, and Deficiencies	6-64
Recommendations with Significant Problems	6-64
Prior Recommendations Not Yet Implemented	65-66
Matters Referred to Prosecutive Authorities	2
Summary of Instances Where Information Was Refused	N/A
Listing of Audit Reports	76-87
Summary of Significant Audits	6-64
Reports with Questioned Costs	72-73; 80-87
Reports Recommending That Funds Be Put To Better Use	74
Summary of Reports in Which No Management Decision Was Made	65-66; 72-74
Revised Management Decisions	N/A
Management Decision Disagreements	N/A

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations - Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292 or email DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer.