DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

SEMIANNUAL REPORT TO THE CONGRESS

April 1, 2005 – September 30, 2005

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, 2005

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

Dear Mr. Secretary:

I am pleased to present our semiannual report, which summarizes the activities and accomplishments of the Department of Homeland Security (DHS) Office of Inspector General for the six-month period ending September 30, 2005.

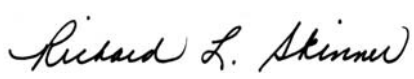
During this reporting period, our office issued 34 management reports (audits and inspections). In addition, we issued 23 audit reports on grants and contracts, and processed 183 reports on DHS programs that were issued by other organizations. As a result of these efforts, $31.1 million of questioned costs were identified, of which $8.1 million were determined to be unsupported. Additionally, audit recoveries totaled $13.6 million. I am most proud, however, of the positive response our reports have received from departmental management. This is demonstrated by the fact that management has concurred with over 90% of our recommendations.

In the investigative area, we issued 246 reports. Our investigations resulted in 54 arrests, 70 indictments, and 66 convictions. Our investigators closed 279 investigations and 5,341 complaints received though the hotline. Additionally, investigative recoveries, fines, and restitutions totaled $2.2 million.

As we close this reporting period, the Department faces an unprecedented challenge continuing to focus on its mission, while coordinating recovery efforts from Hurricane Katrina, the costliest natural disaster in our nation's history. Our office has already initiated efforts, in coordination with inspectors general from throughout government, to

assist program managers in ensuring the billions of dollars in funds targeted to support that effort are spent wisely and in the most effective manner possible.

Sincerely,



Richard L. Skinner
Inspector General

TABLE OF CONTENTS

STATISTICAL HIGHLIGHT OF OIG ACTIVITIES
April 1, 2005 – September 30, 2005

Dollar Impact	
Questioned Costs…….	$31,106,976[1]
Funds Put to Better Use……..……	$0
Management Agreement That Funds Be:	
Recovered.....	$0
De-obligated.....	$0
Funds Recovered (Audit & Investigative).....	$15,299,779
Fines and Restitutions.....	$579,973
Administrative Cost Savings and Recoveries.....	$0
Activities	
Management Reports Issued …….....	34
Investigation Reports Issued …….....	246
Grant and Contract Audit Reports Issued…..…….....	23
Single Audit Reports Processed.....	100
Defense Contract Audit Agency.....	83
Investigations Initiated.....	490
Investigations Closed.....	279
Open Investigations.....	1,341
Investigations Referred for Prosecution.....	103
Investigations Accepted for Prosecution.....	28
Investigations Declined for Prosecution.....	26
Arrests.....	54
Indictments.....	70
Convictions.....	66
Personnel Actions.....	24
Total Complaints Received.....	4,680
Total Hotlines Received.....	2,919
Complaints Referred (to programs or other agencies).....	3,859
Complaints Closed.....	5,341

[1]The questioned costs represent those costs identified by our Office ($13,478,172) and non-Federal auditors, i.e., DCAA ($16,336,559) and independent accounting firms for single grant audits ($1,292,245).

EXECUTIVE SUMMARY

This is the sixth 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, 2005, to September 30, 2005. 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 34 management reports (Appendix 3) and 246 investigative reports. Additionally, we issued 23 grant and contract audit reports, and processed 183 reports on DHS programs - 83 audits issued by the Defense Contract Audit Agency (DCAA), and 100 single grant audits which were 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 efficiency, effectiveness, and economy of the respective program.

During this reporting period audits, inspections, and investigations resulted in questioned costs of $31,106,976, of which $8,118,945 was determined to be unsupported costs. Additionally, recoveries, restitutions, and fines totaled $15,879,752. Our investigations resulted in 54 arrests, 70 indictments, and 66 convictions. Moreover our investigators closed 279 investigations and 5,341 complaints received through the hotline.

We have a dual reporting responsibility to Congress as well as to the Secretary. During the reporting period, we continued our active engagement with Congress through numerous meetings, briefings, and dialogues with members and staff of the Department's authorizing and appropriations committees and subcommittees on a range of issues relating to our work and that of the DHS. We also testified before Congress on eight occasions during this reporting period. Our testimonies can be read on our website's congressional testimony link at www.dhs.gov.

DEPARTMENT OF HOMELAND SECURITY PROFILE

On November 25, 2002, President Bush signed the *Homeland Security Act* (Public Law 107-296, as amended), officially enabling 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. response to national emergencies.

The Department has been organized into the following five directorates:

Border and Transportation Security
Science and Technology
Information Analysis and Infrastructure Protection
Emergency Preparedness and Response
Management

Other critical components of DHS include the:

United States Coast Guard
United States Secret Service
United States Citizenship and Immigration Service
Office of State and Local Government Coordination and Preparedness

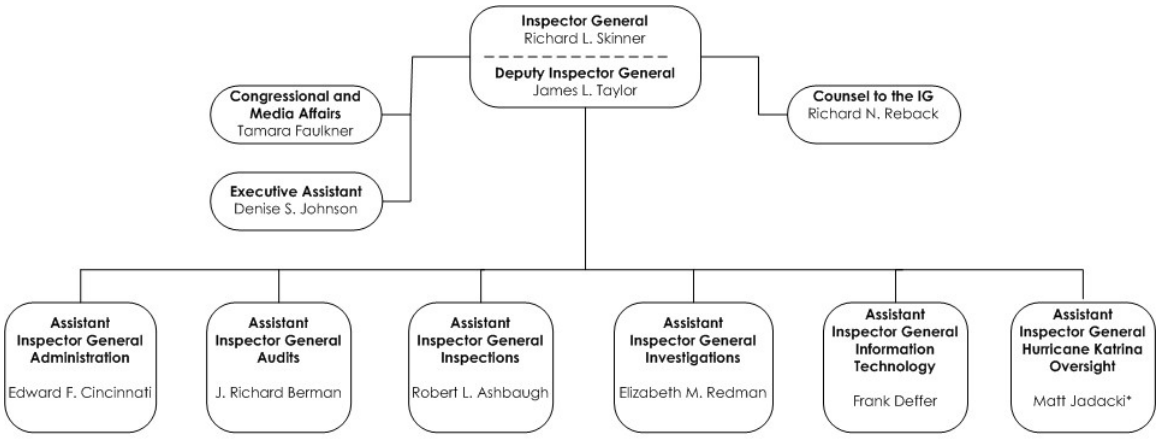
OFFICE OF INSPECTOR GENERAL PROFILE

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 502 full-time employees and approximately 40 temporary employees to provide audit and investigations oversight of Hurricane Katrina operations. We are comprised of six functional components. We are based in the District of Columbia and have 26 field offices throughout the country. We have also opened temporary offices at each of the four joint field offices established by the Federal Emergency Management Agency (FEMA) to administer Hurricane Katrina disaster relief programs.

Department of Homeland Security
Office of Inspector General
Management Team



* on detail from Department of Commerce

SUMMARY OF SIGNIFICANT OIG ACTIVITY

HURRICANE KATRINA OVERSIGHT

On September 28, 2005, we testified before the House Energy and Commerce Subcommittee on Oversight and Investigations on the IG community's plans for Hurricane Katrina oversight. Congress had passed legislation that provided over $63 billion to DHS for disaster relief, including $15 million for us to oversee the management and expenditure of those funds. Although the FEMA is responsible for coordinating response and recovery efforts, it will take the combined efforts of many federal, state, and local government entities to restore the Gulf Coast. Therefore, the oversight task encompasses more the just our office. The circumstances created by Hurricane Katrina provided an unprecedented opportunity for fraud and mismanagement, and some estimate that the cost to recover from the storm and rebuild the affected areas could reach $200 billion and more.

In addition to its own activities related to Hurricane Katrina, FEMA tasked other federal departments and agencies through Mission Assignments. As of September 30, 2005, FEMA had made mission assignments totaling just over $7 billion, over $6 billion of which went to the Department of Defense (DOD) and the Army Corps of Engineers. Departments use mission assignment funds to award contracts or provide direct support for response efforts. In addition, some departments and agencies, including DOD, received direct appropriations for Hurricane Katrina activities. We expect more disaster relief funds and direct appropriations for Katrina relief in the weeks and months ahead.

To answer the call for oversight in the face of this unprecedented disaster, and to ensure that our office and other IGs work together to coordinate our efforts, I have created a new Office of Hurricane Katrina Oversight, lead by an assistant IG. We are collectively focused on our departments' and agencies' response and recovery efforts and the related disaster assistance spending. The overriding objective of the OIGs' plans is to ensure accountability and preventing problems before they occur. Our plans focus heavily on prevention, including reviewing internal controls; monitoring and advising department officials on contracts, grants, and purchase transactions before they are approved; and meeting with applicants, contractors, and grantees to advise them of the applicable federal laws and regulations governing the use of disaster relief funds, and to assess their capability to account for the funds. The plans also encompass an aggressive and ongoing audit and investigative effort designed to ensure that disaster relief funds are being spent wisely and to identify waste, fraud, and abuse as early as possible.

BORDER AND TRANSPORTATION SECURITY

Transportation Security Administration (TSA)

Transportation Security Administration's Revised Security Procedures
In response to a request from the U.S. House Committee on Government Reform, our office conducted a review of procedures initiated by TSA in response to the security breaches experienced in 2003 on Southwest Airlines aircraft. We assessed TSA's changes to procedures used by its Contact Center for handling emails and other correspondence, and any changes related to the inspection of aircraft. We recommended that TSA (1) establish a process to regularly review and evaluate how timely Contact Center personnel handle the communications and implement additional corrective actions, as needed; (2) revise its security directive to require air carriers to retain aircraft security search documentation; and (3) require that, as part of the annual work plan, each federal security director's inspector workforce personally observe a random sample of aircraft searches and review search documentation. The findings and recommendations were presented to the committee in a sensitive security information report. (OIG-05-51, September 2005, OA)

Transportation Security Administration's Procedures for Law Enforcement Officers Carrying Weapons on Board Commercial Aircraft
The Ranking Democratic Member, Committee on Transportation and Infrastructure, requested that we determine whether current TSA operating procedures ensure the safe and secure transport of weapons on commercial aircraft by law enforcement officers. Further, the Congressman also asked us to report the number of federal, state, and local officers authorized to carry weapons on commercial aircraft.

TSA procedures to verify the identity of law enforcement officers, flying armed, need to be strengthened. In addition, TSA should establish procedures to manually inspect a random sample of officers' carry-on bags and ask the officer, during processing, if they are carrying hazardous materials such as pepper spray or mace in their carry-on bags. Although the U.S. Department of Justice estimates there are over 801,000 federal, state, and local officers, the number authorized to fly armed is unknown. The *Intelligence Reform and Terrorism Prevention Act of 2004* mandated improved verification of officers flying armed, by requiring TSA to begin issuing a uniform biometric credential to all federal, state, and local officers within 120 days (or by April 16, 2005) of enactment. In July 2004, TSA's credentialing program office launched a Registered Armed LEO Pilot program to establish a uniform credential with biometric identification technology. TSA stated that it met the minimum required by the congressional mandate through its pilot program. However, the pilot program does not fully address the requirements in this Act, since TSA is still testing off-the-shelf technology by two contractors; and, it has not

selected the type of uniform biometric credential to be used and it has not developed a comprehensive plan necessary to implement a credential.

We recommended that TSA (1) expedite selection of the uniform biometric credential to be used, and develop and implement a comprehensive plan of action to identify the work to be completed, milestone completion dates, project cost, and funding; and, (2) revise operating procedures to require that law enforcement officers' carry-on bags be manually inspected before the officer enters the sterile area of the airport, at least until a uniform biometric credential is in place. (OIG-05-52, September 2005, OA)

Independent Auditor's Report on TSA's FY 2004 Financial Statements
Because of TSA's request for a "stand-alone" financial statement audit, we engaged the independent accounting firm KPMG LLP to audit TSA's fiscal year (FY) 2004 financial statements, in conjunction with the audit of DHS' FY 2004 financial statement audit. KPMG issued an unqualified opinion on TSA's FY 2004 financial statements and identified two material weaknesses related to IT and internal control monitoring. KPMG noted weaknesses with respect to IT security management and system integration at TSA's financial system service provider, and significant errors in personnel records that TSA had identified and was working to correct. KPMG noted that TSA's process to identify internal control weaknesses was not sufficient to meet the requirements of the *Federal Managers' Financial Integrity Act* and the Office of Management and Budget's (OMB) implementing guidance. KPMG identified an additional reportable condition related to grants management. (OIG-05-40, September 2005, OA)

Improved Security Required for Transportation Security Administration Networks
We audited DHS' security program and its organizational components to determine the effectiveness of controls implemented on selected wired-based sensitive but unclassified networks. This audit included a review of applicable DHS and TSA security policies, procedures, and other appropriate documentation. In addition, we performed vulnerability assessments to evaluate the effectiveness of controls implemented on selected network devices.

TSA has taken actions and made progress in securing its networks. TSA has also strengthened the security configurations on its servers and workstations. As a result, we detected significantly fewer security vulnerabilities compared to the vulnerability assessment results reported in a prior OIG audit report.

However, TSA can make further improvements to secure its networks. For example, TSA has not developed adequate policies and procedures, or fully implemented processes that address security testing, monitoring network activities with audit trails, and configuration and patch management. In addition, the contingency plan for the TSANet has not been

finalized and tested to ensure that critical operations could be restored in the event of emergency.

We made several recommendations that would help TSA improve its network management and security controls and ultimately better protect the confidentiality, integrity, and availability of sensitive information. TSA agreed with our conclusions and has already taken steps to implement each of the recommendations. (OIG-05-31, August 2005, IT)

TSA Screeners Charged with Theft
We investigated an allegation that two TSA screeners had been stealing items from passengers' luggage while on duty. During our interviews, both admitted that they had been stealing from passengers' luggage for several months. We recovered some of the stolen items, which included laptop computers, digital cameras, DVD players, and camcorders. In November 2004, both screeners resigned from TSA pending termination. In August 2005, target letters from the United States Attorney's Office were delivered to the two former screeners for violating 18 USC §654, Theft by Government Employees. (OI)

Two TSA Security Screeners Charged with Theft of Prescription Medications (Update)
In November 2004, we conducted an undercover operation targeting screeners at an airport who allegedly had been stealing prescription medications from wheelchair bound passengers. One TSA screener was arrested for stealing oxycontin pills from an undercover agent's carry-on bag. The screener confessed and admitted to stealing other passengers' prescription medications on approximately twenty or more occasions since June 2004. Also, a second TSA screener and co-conspirator confessed to stealing prescription medications from passengers' carry-on bags on five separate occasions and was subsequently arrested. On December 10, 2004, the United States Attorney's Office charged both TSA security screeners with 18 USC §654, an Officer or Employee of United States Converting Property of Another, and 21 USC §844, Possession of Schedule II Narcotics Without a Prescription. In February 2005, both TSA security screeners resigned in lieu of termination. In September 2005, the U.S. Attorney's Office sent target letters to the TSA security screeners' attorneys, with an attached proposed Information charging them with one count of 18 USC §654; Employee of the United States Converting Property of Another. (OI)

U.S. Immigration and Customs Enforcement (ICE)

DHS' Responsibilities for Juvenile Aliens
We reviewed the effectiveness of the coordination between Customs and Border Protection (CBP) and ICE after CBP apprehends and initially holds juvenile aliens. Our review included the process by which CBP informs the ICE Detention and Removal

Operations (DRO) that a juvenile alien was apprehended, the process for transferring the juvenile alien to ICE DRO custody, and the effectiveness of the current system for transferring care and custody of unaccompanied juvenile aliens to the Department of Health and Human Services. Finally, we assessed the progress of relevant DHS components in implementing three open recommendations from a prior Department of Justice, OIG report.

We concluded that DHS adhered to its responsibilities for treating apprehended juvenile aliens with dignity and concern. The department is proficient in key areas of apprehending and processing juvenile aliens, prioritizing processing and transportation of juveniles after they are apprehended, and providing appropriate information to juveniles on their legal rights. Generally, the department placed juvenile aliens in longer-term housing facilities in a timely manner.

While our overall assessment for this review is satisfactory, areas needing departmental attention include:

- CBP personnel generally provided adequate access to counsel for apprehended juvenile aliens. However, information on lists of pro bono attorneys given to juveniles was not consistently accurate.
- The time which juvenile aliens spent in confinement at CBP facilities varied significantly. There is no CBP-wide policy for reviewing and approving the extended holding of juveniles and for reporting these events to appropriate CBP officials.
- Accompanied juveniles (those apprehended with their families) were separated from their families due to space limitations in "family unity" shelters.
- DHS and the Department of Health and Human Services have not forged a sufficiently detailed agreement on their respective responsibilities for unaccompanied juvenile aliens.
- DHS has not clearly assigned the authority for overseeing the range of its responsibilities for juvenile aliens and for serving as an organizational liaison.
- Training programs delineated in the Flores Stipulated Settlement Agreement are insufficiently implemented and custodial records for juveniles continue to be irregularly completed and maintained.

We made eight recommendations to the Undersecretary, Border and Transportation Security, to improve the management of the juvenile alien program.
(OIG-05-45, September 2005, ISP)

Chain-of-Command for Immigration Enforcement Agents Needs to be Clarified
Under the former Immigration and Naturalization Service (INS), Detention Enforcement Officers (DEOs) performed transportation duties at Border Patrol stations and reported to

Border Patrol supervisors. When DHS was established, these INS operations were reorganized. The Border Patrol moved into CBP, while enforcement operations, including DEOs, moved into ICE. However, some DEOs, now called Immigration Enforcement Agents (IEAs), did not relocate to ICE, but remained with the Border Patrol and continued to perform their legacy transportation duties. They continued to report to Border Patrol supervisors too.

The IEAs were never formally detailed or reassigned to the Border Patrol. ICE continues to pay federal salaries and benefits for these IEAs; however, the ICE DRO does not provide daily supervision, handle employee-relations issues, or handle adverse actions for IEAs reporting to Border Patrol supervisors. At the same time, Border Patrol supervisors do not have the authority to handle employee-relations issues or discipline IEAs who report to them. This has resulted in problems for both the IEAs involved and the Border Patrol supervisors to whom they report. The IEAs who currently report to Border Patrol supervisors need a corrected reporting chain to ICE, or in the alternative, need to be detailed or reassigned to CBP. Also, management needs to clarify the organizational assignment of transportation responsibilities and the expected range of duties of IEAs. (OIG-05-24, June 2005, ISP)

Immigration and Customs Enforcement's Compliance Enforcement Unit
We conducted this review to determine the efficiency and effectiveness of the Compliance Enforcement Unit (CEU) in identifying, locating, and apprehending aliens who have violated the purpose and terms of their admission into the United States. Based on our review of the number of cases referred to CEU and the procedures and systems used to collect, analyze, and process these referrals, we identified several deficiencies in the CEU process.

CEU depends on systems that are incomplete. For example, the most ambitious, United States Visitor and Immigrant Status Indicator Technology (US-VISIT), does not have an established exit control capability at this time,. These systems produce many "leads" that are incomplete or inaccurate and, therefore, are not actionable. In our test sample of leads closed by CEU, 96 percent of the leads proved to be invalid.

The deficiencies in the systems and other factors in the apprehension and removal process result in a minimal impact in reducing the number of overstays in the United States. From January 2004 to January 2005, CEU received 301,046 leads from US-VISIT, SEVIS, NSEERS, and the Department of State. CEU processed 142,816 of these leads. CEU closed 138,652 because it determined the alien had left the United States or was "in status," or the information was insufficient to make apprehension likely. Of the 142,816 leads, CEU referred 4,164 to the field. These resulted in 671 apprehensions. Other studies suggest that very few of the 671 aliens apprehended will actually be removed unless they also have a criminal history and are detained. This output is too

small to affect the estimated annual growth in the undocumented alien population, or the estimated number of overstays in the United States.

There are business practices that CEU can improve. Of the 14,495 US-VISIT, SEVIS, and NSEERS referrals that we examined, CEU had not completed the processing of 7,053 (49%) of these leads in a two-month period, because it was unable to keep pace with the large volume of lead referrals and because not all referral data were actionable.

CEU did not process all violator leads that it did complete in a timely manner due to vague performance measures and processing inefficiencies. As a result, violators have a greater chance to avoid apprehension and disappear into the U.S. population because addresses and other locator information for aliens can be perishable.

Finally, two procedural issues hinder CEU's ability to adequately document and consistently process violator leads. CEU did not: (1) establish the basis for closing over half of the leads in our test sample; and (2) distribute its policies to ICE field offices in an effective manner.

We made four recommendations to CEU to improve its business practices. (OIG-05-50, September 2005, ISP)

ICE's Budgetary Status and Other Areas of Concern

In response to a request from the Ranking Member of the Select Committee on Homeland Security, we engaged the independent accounting firm KPMG LLP to review certain budget related issues pertaining to ICE. Those issues included budget problems at ICE, the adequacy of ICE's Federal Financial Management System (FFMS), travel database disruptions, and procurement tracking difficulties. KPMG reported that they were unable to rely on ICE's processes or financial data to determine its compliance with the *Anti-deficiency Act*; ICE configured FFMS in a way that made funds management more difficult and made certain reports that users needed to do their jobs difficult to access; ICE was unable to make temporary employees in the Office of the Principal Legal Advisor permanent due to insufficient budget resources; travel system operations were disrupted due to shortcomings during its deployment, resulting in delays in processing travel related requests; and procurements were difficult to track due to the lack of integration of the procurement system with FFMS and shortcomings in the procurement structure and process. (OIG-05-32, August 2005, OA)

ICE Agent indicted by a Federal Grand Jury and Pleads Guilty to Theft

We conducted a joint investigation with the Justice OIG and the Federal Bureau of Investigation (FBI) into allegations of theft and other misconduct by an ICE agent assigned as the property officer at a county detention facility. The agent admitted to having stolen some amount of cash from aliens who had been detained at that facility.

Searches were conducted of the agent's residence, government office, several official government vehicles, and two private storage facilities, all of which resulted in the recovery of personal property and valuables belonging to thousands of aliens who had been detained at that facility over a period of several years. As a result of the recovery, analysis of the property, and the interviews of hundreds of current and former alien detainees, evidence was obtained which confirmed the theft of over $300,000 in U.S. currency. The agent was indicted by a federal grand jury and has pleaded guilty to the charge of 18 USC §654, Officer or Employee of the United States Converting Property of Another. The agent is scheduled for sentencing in November 2005. (OI)

Aliens' property seized from agent's residence

Aliens' property seized from agent's residence

Aliens' property seized from agent's residence

Property that was seized from the back of government van assigned to agent

Property recovered from a detention storage facility

Alien property recovered from ICE office at the County Detention Facility

ICE Contract Security Officer Pleads Guilty to Introducing Contraband in a Prison
A contract security officer with ICE pleaded guilty on May 25, 2005, to violations of 18 USC §1791(a)(1) & (b)(3), Providing Contraband in a Prison. The contract security officer was arrested and charged after he solicited and accepted a $1,000 cash bribe and took possession of 83.2 grams of marijuana from an OIG undercover agent. During the undercover meeting, he agreed to smuggle the marijuana into a processing center and deliver it to an ICE detainee. The sentencing has been scheduled for September 27, 2005. (OI)

ICE Officer Charged with Disclosing Information
We initiated an investigation into allegations that an immigration enforcement officer in a DRO office provided information about an ongoing FBI investigation to the subjects of the investigation. Subsequent investigation revealed that the officer was involved in the underlying offense of illegal gambling. On December 16, 2004, the officer was arrested by the OIG and the FBI and charged with 18 USC §1955(a), Illegal Gambling, and 18 USC §371, Conspiracy. In May 2005, the officer plead guilty to one count of 18 USC §371, Conspiracy and resigned from his position. He was sentenced to four years probation and a special assessment of $100. (OI)

Armed Federal Protective Service (FPS) Contract Guard Convicted of Theft
Our investigation of a FPS contract armed guard resulted in his arrest. The guard subsequently was convicted of a felony for stealing cash from visitors while they were undergoing inspection at a checkpoint to a federal building. (OI)

Customs and Border Protection

Vehicle Disposal and Sales Program Within U.S. Border Patrol's San Diego Sector
In response to a request from the U.S. House of Representatives member for the 51st District of California, we audited the fleet vehicle disposal and sales activities of the U.S. Border Patrol's San Diego Sector (the Sector) while under its legacy agency, the INS. The Congressman's request was primarily spurred by a constituent's assertions that (1) vehicles were prematurely disposed of after major restoration work; (2) vehicles were reported as inoperable and downgraded to scrap although the majority were actually in good condition; (3) useable vehicles reported as inoperable or in poor condition were sold to scrap dealers with major components intact; (4) vehicles downgraded to salvage were sold to select individuals and companies at extremely low prices without following traditional sales procedures; and (5) vehicles and heavy-duty equipment were improperly transferred to an Indian Tribe.

We confirmed the validity of the five assertions. The Sector did not manage its aging fleet of vehicles in an effective manner or ensure that the disposal of government assets complied with established policies. It is noteworthy that the Sector was experiencing a severe shortage of serviceable vehicles needed to meet the Border Patrol's operational readiness standards. The Sector's stopgap solution in 2001 resulted in 129 aging vehicles being restored and, as of March 17, 2005, the Sector reported that 69 of those vehicles remained operational in its fleet. CBP now has oversight of the Sector and is working to standardize vehicle fleet management throughout the Bureau; however, to address the deficiencies of the Sector, additional improvements are needed. We made five recommendations to help strengthen controls over the Sector's vehicle fleet. These recommendations may be helpful to CBP as it evaluates how effectively other Border Patrol Sectors are managing their fleet vehicles, and as it implements its Bureau-wide fleet vehicle management system as well. (OIG-05-47, September 2005, OA)

Controls Over the Export of Chemical and Biological Commodities
The *National Defense Authorization Act* requires the OIGs to review the controls over the export of militarily sensitive technologies to countries and entities of concern. We evaluated CBP's enforcement practices to determine whether they are in place and working effectively to prevent the illegal export of chemical and biological commodities. The review is part of a series of interagency OIG reviews on the transfer of militarily sensitive technologies.

CBP does not consistently document the location of licenses issued by the Department of State in its Automated Export System. Exporters physically lodge state licenses with CBP at the port where shipments are expected primarily to occur; however, exports may be made through any authorized U.S. port of exit. Such license information is necessary to

determine whether an individual shipment is being made in compliance with the associated license conditions. When an exporter ships from a port where the state license is not lodged, it becomes difficult for enforcement personnel at the port of shipping to readily obtain license information. As a result, CBP's ability to enforce State licensed exports in a timely and efficient manner is reduced. Also, CBP needs to improve its enforcement of license requirements for shipments that have been processed against commerce licenses.

We recommended that the Commissioner of CBP evaluate the Outbound (Export) Program, including information requirements, staffing needs, and consistency of enforcement practices, and make necessary adjustments to ensure that all of CBP's enforcement responsibilities are accomplished. (OIG-05-21, June 2005, OA)

Targeting Oceangoing Cargo Containers

In response to a congressional mandate in the United States Coast Guard and Maritime Transportation Act of 2004, we reviewed the Automated Targeting System (ATS) used by CBP for selecting ocean-going cargo containers for inspection. Our review also included an overview of oceangoing container supply chain security.

The supply chain can be separated into three major segments: overseas, which includes manufacturing, warehousing, transporting, and loading of the product into a container and on board a ship; transit at sea; and, U.S. ports. Each segment of the supply chain - overseas, transit at sea, and at U.S. ports - presents vulnerabilities, but the overseas segment is the most problematic. This segment is outside the jurisdiction of the U.S. government and includes all initial handling and movement of the containers from the loading of the container (stuffing) to placing the container on-board a U.S. bound vessel. Improved security over this segment of the supply chain requires leveraging the authority of foreign governments through diplomacy.

Using more complete and accurate shipping data and systematically analyzing container examination results to refine existing targeting rules and develop new rules could improve the effectiveness of the ATS. In addition, we found inconsistencies in the examination statistics contained at the ports and CBP headquarters. Additionally, physical controls over containers selected for examination needed improvement.

We made recommendations to improve data to which ATS targeting rules are applied; use the examination results to refine and develop new rules; and, improve the security over containers selected for inspection. (OIG-05-26, July 2005, OA, FOUO)

Improved Security Required for CBP Networks

We audited DHS and its organizational components' security program to determine the effectiveness of controls implemented on selected wired-based sensitive but unclassified

networks. This audit included a review of applicable DHS and CBP security policies, procedures, and other appropriate documentation. In addition, we performed vulnerability assessments to evaluate the effectiveness of controls implemented on selected network devices.

Our objective was to determine whether CBP has implemented adequate controls to protect its networks. CBP shares law enforcement and trade sensitive data through its wide area network (WAN) or Private Internet Protocol WAN. This WAN connects to local area networks (LAN) located throughout the country.

CBP has not developed adequate policies or fully implemented procedures or processes that address security testing, monitoring network activities with audit trails, and configuration and patch management. In addition, CBP has not implemented the necessary controls to ensure that the data residing on and traveling through its network resources is properly protected.

Security controls must be improved in order for CBP to provide adequate and effective security over its networks. Our vulnerability assessments identified security concerns resulting from inadequate password controls, missing critical patches, vulnerable network devices, and weaknesses in configuration management. These security concerns provide increased potential for unauthorized access to CBP resources and data.

We made several recommendations to assist CBP to more effectively secure its networks. Effective network management and security controls are needed in order to protect the confidentiality, integrity, and availability of sensitive information. In response to our draft report, CBP agreed and has already taken steps to implement each of the recommendations. (OIG-05-39, September 2005, IT)

CBP Officer Indicted for Aiding and Abetting

Our investigation of a CBP officer originated following the arrest of a Canadian national on December 22, 2004, for violation of 18 USC §1001, False Statements. The Canadian, a passenger on a bus arriving in the United States from Canada, was arrested after she admitted lying to officials about her criminal history in her attempt to gain entry into the U.S. During a post-arrest interview, she identified the officer as her fiancé and said that he was aware of her criminal history and had instructed her not to mention it when crossing the border.

The officer admitted in an interview with us that he instructed her not to mention her criminal history if questioned at the border, and that he induced her to lie to the judge at her preliminary/detention hearing. A federal grand jury returned a two-count indictment charging the officer with Aiding and Abetting in the smuggling of an alien into the U.S. (OI)

Former Border Patrol Agent (BPA) Sentenced for Attempted Possession With Intent to Distribute Cocaine

On July 22, 2005, a former BPA was sentenced to 70 months in prison and three years supervised release after pleading guilty to attempted possession with intent to distribute cocaine. On December 14, 2004, he was apprehended in an undercover operation after he transported 10 kilograms of cocaine through a U.S. Border Patrol checkpoint in exchange for a payment of $8,000 dollars. This matter was jointly investigated with ICE. (OI)

10 kilograms seized cocaine

Two U.S. BPAs indicted for Intent to Commit Murder, Assault with a Dangerous Weapon and Assault with Serious Bodily Injury

As a result of our investigation, two U.S. BPAs were arrested on March 18, 2005, and subsequently indicted by a federal grand jury on April 13, 2005, after discharging their firearms and causing serious bodily injury to a suspected marijuana trafficker who was allegedly unarmed and in the process of fleeing when the shooting occurred. A trial date has been set for October 17th in United States District Court. If convicted, each faces a possibility of up to 40 years in prison and/or fines up to a maximum of $750,000. (OI)

CBP Officer Found Guilty of Conspiracy

A CBP officer was found guilty during a jury trial of Conspiracy to Commit Alien Smuggling and Conspiracy to Make False Passports. We pursued anonymous information and the officer was observed assisting a Dominican national in the smuggling of two undocumented aliens from the Dominican Republic through the airport. We identified multiple previous flights, all worked by the officer, on which the Dominican national smuggler had traveled. Examination of the customs declaration forms for the passengers from these flights revealed forms for Dominican citizens, all processed by the officer, for which there were no appropriate immigration entries. The Dominican national smuggler also has been arrested, convicted, and sentenced. The officer is currently awaiting sentencing. (OI)

BPAs involved in Alien Smuggling

We initiated an investigation after receiving information from a Narcotics Task Force that BPAs were involved with a drug smuggling organization based in San Diego County. Information obtained disclosed that one of the drug smuggling organization's members was in contact with a BPA assigned to the Border Patrol San Diego Sector. Our investigation identified two BPAs who were involved in smuggling illegal aliens into the United States. Both agents were indicted and arrested. One of the agents admitted that they were charging the aliens up to $2,000 per alien for guaranteed entry into the U.S. On several occasions, Border Patrol service vehicles were used in smuggling the aliens. Additionally, our investigation revealed that one of the agents is in fact an illegal alien who used false documents to enter the U.S. Navy and the U.S. Border Patrol. Both agents are currently in judicial proceedings. (OI)

Port Director Accepted Bribes for Release of Law Enforcement Information and Failed to Report Subordinate involved in Smuggling Activity

We initiated an investigation after receiving information from a former INS inspector that an airport area port director had accepted bribes in return for sensitive law enforcement information. The former INS inspector was indicted and arrested for accepting bribes from a smuggling organization to facilitate the smuggling of illegal aliens and narcotics. The Port Director was arrested, indicted, and removed from her position as Port Director. Judicial proceedings are pending. (OI)

Bribery and Alien & Narcotics Smuggling

An investigation was initiated after we received information that an INS inspector was accepting bribes from a Mexican-based smuggling organization. Between 1999 and 2002, he was given over $500,000 by the smuggling organization. In return, he allowed numerous vehicles laden with illegal aliens and narcotics into the U.S. through the Port of Entry. He resigned during 2002 after being warned of this investigation by a former assistant area port director. He and eight members of the smuggling organization were indicted and arrested. Between May and August 2005, three members of the smuggling organization pled guilty to several counts of conspiracy, use of false immigration documents and smuggling illegal aliens. Judicial proceedings are pending against the INS inspector. (OI)

CBP Officer Accused of Selling Fictitious U.S. Immigration Documents to Illegal Aliens (Update)

A CBP officer in the United States Virgin Islands was accused of selling fictitious U.S. immigration documents to illegal aliens. Our investigation determined that the officer was engaged in a criminal conspiracy, with eight co-defendants, to provide fictitious U.S. immigration documents to illegal aliens. The officer was convicted of document fraud and sentenced to 41 months confinement and 36 months supervised probation. Six

defendants received varying sentences and one defendant has not yet been sentenced. (OI)

Attempted Bribe of a BPA
We received an allegation that a Mexican chief of police had attempted to bribe a CBP BPA to allow vehicles laden with marijuana to enter the United States. We conducted an investigation in conjunction with the Border Patrol, FBI Corruption Task Force and ICE.

On April 20, 2005, a federal grand jury indicted the Mexican chief of police and his police officer co-conspirator in a two-count indictment. Count one charges violations of 18 USC §201(b)(1)(C), Bribery of a Public Official and 18 USC §2, Aiding and Abetting; and count two charges violations of 21 USC §841 (a)(1); 21 USC §841 (b)(1)(A)(vii), Possession with Intent to Distribute Marijuana, and 21 USC §846, Conspiracy to Possess with Intent to Distribute Marijuana. Both defendants are pending trial. (OI)

Export Brokers Plead Guilty to Felony Gratuities, Bribery; Five Remain Wanted
The semiannual report to Congress, April 1, 2004 – September 30, 2004, included a summary of a seven-month undercover investigation that yielded the arrests of 18 vehicle export brokers and one National Insurance Crime Bureau employee. The employee was sentenced to 3 months confinement and 3 years supervised probation. Eleven of the export brokers pleaded guilty to felony gratuities or bribery; arrest warrants for five export brokers were issued for failing to appear in court. Two export brokers have trials scheduled for October 2005. (OI)

BPA Canine Handler and his Brother Plead Guilty to Bribery and Conspiracy to Possess with Intent to Distribute Marijuana and Cocaine
Our investigation, conducted jointly with the FBI and Drug Enforcement Agency, determined that a BPA canine handler and his brother sought, received and accepted approximately $1.5 million dollars in bribe money to allow safe passage of several narcotic shipments through a Texas Border Patrol Checkpoint. The United States Attorney's Office, Southern District of Texas, prosecuted the case. The agent canine handler and his brother plead guilty to two of thirteen counts of the indictment and are presently awaiting sentencing. The canine handler was terminated from his position. (OI)

CBP Inspector Pleads Guilty to Making False Statements
We conducted an investigation involving a CBP supervisory inspector assigned to a port of entry. The investigation determined that the supervisory inspector was involved in the sale of immigration documents to non-qualifying aliens. On March 28, 2005, a grand jury returned an indictment in relation to the criminal scheme. On May 3, 2005, the supervisory inspector was arrested pursuant to the indictment and subsequently pleaded guilty to giving false statements to OIG agents who had interviewed him during the

course of the investigation. The inspector's employment was terminated and he presently awaits sentencing. (OI)

EMERGENCY PREPAREDNESS AND RESPONSE (EP&R)

We issued 23 grant audit reports, including 17 audit reports of disaster sub-grants valued at about $213 million. In addition, we audited Pennsylvania, the District of Columbia, Florida, New Hampshire, and Vermont's administration of their grant relief programs and concluded that certain financial and management controls were needed. We questioned a total of $13,478,172 costs, of which $3,975,303 was unsupported.

An itemized list of the audit reports that include questioned or unsupported costs are enveloped in Appendix 4.

FEMA's Individuals and Households Program in Miami-Dade County, Florida, for Hurricane Frances

We sought to determine whether FEMA had sufficient evidence to support the county's eligibility for Individuals and Households Program (IHP) assistance and whether adequate program controls existed to ensure that funds were provided only to eligible applicants, for eligible expenses.

The administration of the IHP has two key control points: (1) the disaster declaration and related amendment process, which is designed to assess damages and losses and determine and document the need for a major disaster declaration and FEMA assistance; and (2) the inspection of damages and verification of losses reported by individuals and households to determine whether the losses are disaster-related and eligible for FEMA assistance. Our review of the IHP in Miami-Dade disclosed shortcomings in both areas.

- FEMA designated Miami-Dade County eligible for the Individual Assistance program without a proper preliminary damage assessment;
- Funds provided for repairs and replacement of household room items were not based on actual disaster-related damages or losses;
- The verification of some personal property damages or losses were based on undocumented verbal representations;
- Guidance and criteria for replacing and repairing of automobiles and the reimbursement of expenses for funerals and other items were generally lacking; and,
- Some Expedited Rental Assistance awards were made to some applicants without reasonable assurance of eligibility.

Further, FEMA's oversight of inspections needs improvement. Specifically contractors were not required to review inspections prior to submission; edit checks for inspection errors were made after payment rather than before; and, no provisions existed for inspectors to recuse themselves from inspections that may have presented possible conflicts of interest.

The policies, procedures, and guidelines used in Miami-Dade County for the IHP were used throughout the State of Florida, casting doubt about the appropriateness of IHP awards made to individuals and households in other counties of the state as a result of the four hurricanes, particularly those counties that had only marginal damage. Further, according to FEMA officials, most of the procedures were used for disasters in other states making the conditions and recommendations broadly applicable to FEMA's implementation of the IHP nationwide. (OIG-05-20, May 2005, OA)

Columbia Space Shuttle Mission Assignment National Forests and Grasslands in Texas, Lufkin, Texas

We audited mission assignment funds awarded to the United States Department of Agriculture, Forest Service (Forest Service) to determine whether it accounted for and expended FEMA funds according to federal regulations and FEMA guidelines. The Forest Service received an award for four mission assignments with obligated funds totaling $151.9 million from FEMA for search and recovery activities related to the February 2003 breakup of the Columbia Space Shuttle. As of September 10, 2003, the Forest Service had billed FEMA $105.7 million for expenses incurred under two of the four mission assignments. We examined 43 percent of these expenses.

The Forest Service did not account for FEMA funds according to federal regulations and FEMA guidelines. Further, weaknesses in Forest Service financial management systems limited our ability to determine whether the Forest Service expended FEMA funds according to these same regulations and guidelines. We recommended that the regional director, FEMA Region VI, disallow $3,415,340 of questionable costs, require the Forest Service to validate and provide documentation to support all billings for those categories with questioned costs, and develop and implement effective property management procedures for use during mission assignments in accordance with the Federal Response Plan. (DD-05-05, April 2005, OA)

Municipality of Coamo, Puerto Rico

The municipality received an award of $3.8 million from the Puerto Rico Office of Management and Budget to remove debris, provide emergency protective measures, and repair roads and other public facilities damaged as a result of Hurricane Georges. The municipality's claim included questioned costs of $1,031,165 ($928,048 FEMA share), resulting from excessive, unsupported, duplicative costs and work that was not completed. (DA-22-05, August 2005, OA)

Monroe County School District, Key West, Florida
The district received an award of $6.5 million from the Florida Department of Community Affairs to remove debris and repair or replace buildings damaged as a result of Hurricane Georges. We questioned costs of $548,035 ($411,026 FEMA share) resulting from charges that were either excessive or covered by insurance. (DA-17-05, June 2005, OA)

City of Columbus, Mississippi
The city received an award of $5.6 million from the Mississippi Emergency Management Agency to remove debris, provide emergency protective measures, and restoration of facilities damaged as a result of severe storms in February 2001. We questioned costs of $256,770 ($192,578 FEMA share) resulting from either unsupported or improper, or not reduced by applicable credits. (DA-16-05, May 2005, OA)

Central Rural Electric Cooperative, Inc., Stillwater, Oklahoma
We audited public assistance funds awarded to the Central Rural Electric Cooperative (CREC), located in Stillwater, Oklahoma. The objective of the audit was to determine whether CREC accounted for and expended FEMA funds according to federal regulations and FEMA guidelines.

CREC received an award of $5.45 million from the State of Oklahoma, Oklahoma Department of Civil Emergency Management (ODCEM), a FEMA grantee, for damages caused by a severe winter ice storm during the period January 30, 2002, through February 11, 2002. The award provided 75 percent FEMA funding for three large projects. We audited all projects under the award. The audit covered the period January 30, 2002, to May 13, 2004, during which CREC claimed $5.45 million and ODCEM disbursed $4.77 million in FEMA funds for direct program costs.

CREC did not account for or expend FEMA funds according to federal regulations and FEMA guidelines. Specifically, CREC awarded non-competitive time-and-materials contracts for $3,239,787 that did not comply with federal procurement standards. As a result, fair and open competition did not occur and FEMA has no assurance that contract costs claimed were reasonable. Further, we questioned $1,875,324 ($1,406,493 FEMA share) of the total $5,449,499 claimed (34.41%) for costs related to improperly procured contracts ($1,802,562) and ineligible materials costs ($72,762). (DD-06-05, May 2005, OA)

Management Issues Identified During the Audit of Texas' Compliance With Disaster Assistance Program's Requirements
Our audit identified certain rule violations and weaknesses in internal controls, but concluded that the State of Texas, for the most part, had effectively managed FEMA disaster assistance program funds in accordance with federal requirements. During the

audit, we identified four additional conditions that required FEMA Region VI's attention. Specifically, FEMA Region VI: (1) did not properly prepare, review, and approve Requests for Assistance for one disaster; (2) improperly waived the requirement for Public Assistance Quarterly Progress Reports; (3) gave improper guidance on reporting the non-federal shares of Public Assistance project costs; and, (4) did not aggressively pursue recovery of duplicate benefits awarded to Individual and Family Grant Recipients. (DD-07-05, June 2005, OA)

Kiamichi Electric Cooperative, Inc., Wilburton, Oklahoma

We audited public assistance funds awarded to the Kiamichi Electric Cooperative, Inc., located in Wilburton, Oklahoma. The objective of the audit was to determine whether Kiamichi accounted for and expended FEMA funds according to federal regulations and FEMA guidelines.

Kiamichi received an award of $9.65 million from the State of Oklahoma, ODCEM, a FEMA grantee, for damages caused by an ice storm on December 25, 2000. The award provided 100 percent FEMA funding for six large projects and 75 percent FEMA funding for one large project and five small projects. The audit covered the period December 25, 2000, to September 6, 2001, during which Kiamichi claimed $9.65 million and ODCEM disbursed $8.34 million in direct program costs.

Kiamichi did not account for or expend FEMA funds according to federal regulations and FEMA guidelines. Specifically, Kiamichi did not follow federal procurement standards in awarding $8,381,786 of contract work. As a result, fair and open competition did not occur and contract costs were excessive. Further, we identified questioned costs totaling $6,235,687 ($5,657,548 FEMA share), or 65 percent of the $9,649,393 claimed. **(**DD-08-05, July 2005, OA)

Western Farmers Electric Cooperative, Anadarko, Oklahoma

We audited public assistance funds awarded to Western Farmers Electric Cooperative (WFEC), Anadarko, Oklahoma. The objective of the audit was to determine whether KiamWFEC expended and accounted for FEMA funds according to federal regulations and FEMA guidelines.

WFEC received an award of $2.05 million from the Oklahoma Department of Emergency Management, a FEMA grantee, for damages resulting from a severe ice storm beginning on December 25, 2000 and ending January 10, 2001. The award provided funding for three large projects: one project for emergency work funded at 100 percent and two projects for permanent work funded at 75%. We examined all projects under the award. The audit covered the period December 25, 2000, to December 2, 2002 during which WFEC claimed $2.05 million and the emergency management department of Oklahoma disbursed $1.6 million in direct program costs.

WFEC did not expend and account for all FEMA funds according to federal regulations and FEMA guidelines. WFEC did not comply with federal procurement standards or FEMA guidelines in awarding $592,643 of contracted utility and debris removal work. Further, WFEC's claim included $259,851 ($245,901 FEMA share) of costs that we found questionable. The questioned costs included ineligible damages to private property ($204,049), overstated fringe benefits ($34,098), duplicate labor costs ($15,984), and unsupported costs ($5,720). (DD-09-05, September 2005, OA)

City of San Jose, California

The City received a public assistance grant award of $3.23 million from the California Office of Emergency Services for facilities damaged as a result of the February 1998 flooding. We identified $349,713 ($262,285 FEMA share) in unsupported, ineligible, and unallowable costs. (DS-13-05, July 2005, OA)

Emergency Preparedness and Response Could Better Integrate Information Technology with Incident Response and Recovery

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

We conducted an audit of the information and technology that Emergency Preparedness and Response (EP&R) uses to support incident management. The objectives of the audit were to (1) review the directorate's approach for responding to and recovering from terrorist attacks, major disasters, and other domestic emergencies; (2) determine the effectiveness of guidance and processes to support IT users during incident management; and, (3) evaluate existing and proposed systems and other technologies used to accomplish EP&R's response and recovery mission.

The EP&R Chief Information Officer (CIO) is making progress with respect to IT planning, including the development of the agency's first IT strategic plan. However, while the IT plan aligns with FEMA's outdated strategic plan, it does not reflect FEMA's integration into DHS and therefore may not support DHS' strategic goals. Further, EP&R CIO support to IT users could be improved. Additional guidance and training for systems users is necessary to ensure that they have the knowledge and information needed to perform their jobs.

Currently, EP&R systems are not integrated and do not effectively support information exchange during response and recovery operations. Also, EP&R has not fully updated its enterprise architecture to govern the IT environment. EP&R would benefit from

strategically managing IT by aligning its IT planning with DHS' direction as well as ensuring systems users receive more timely training and communication.

We made several recommendations for EP&R to use IT more effectively to support response and recovery activities. Updates to both the FEMA and the IT strategic plans are needed. Also, FEMA's business and system requirements should be developed and maintained, and used as the basis for IT alternative analysis. Lastly, an adequate test environment should be developed, maintained, and used to thoroughly test systems prior to their release. The EP&R CIO neither concurred nor non-concurred with our recommendations, but instead provided additional detailed comments and information to update or supplement issues we outline in our report. (OIG-05-36, September 2005, IT)

Challenges in FEMA's Flood Map Modernization Program

Floods are among the most frequent and costly of all natural disasters and have great impact in terms of economic and human losses each year. Since 1978, FEMA has been charged with assisting communities by producing flood maps that detail areas at risk; identify where flood insurance is needed; and, help limit construction within flood zones. However, the majority of FEMA's maps are outdated and in unalterable paper format. In response to demands for more accurate mapping products, FEMA has embarked on a six-year, $1.475 billion program to update and digitize the nation's flood maps. We conducted an audit to assess FEMA's management approach; coordination with federal, state, and local entities; and, acquisition and use of technology to meet map modernization program objectives.

We determined that while FEMA is making progress in map modernization, a number of significant challenges remain. Specifically, FEMA has developed a plan that outlines the priorities, resources, and standards for accomplishing map modernization in communities across the U.S. However, because of budget limitations, FEMA's plan does not reflect user or funding needs. Also, the plan does not provide guidance on how new mapping standards will be achieved. Due to these deficiencies, the plan discourages stakeholder buy-in and may not help FEMA meet its map modernization schedule and quality goals.

Further, FEMA has enhanced its efforts to partner and communicate with its mapping stakeholders, but the agency has not maximized the benefits possible through these relationships. Additionally, as part of its map modernization efforts, FEMA is developing a web-based technology platform and tools to support efficient production and sharing of digital maps. However, FEMA's IT development approach has limited program progress; unclear contractor expectations; underestimation of program scope and complexity; and, poorly defined requirements, which have resulted in significant system acquisition delays and cost overruns.

We recommended that FEMA review and revise the Multi-Year Flood Hazard Plan as well as improve program guidance, contractor oversight, and coordination with stakeholders. Also, FEMA should develop adequate requirements, clearly define contractor expectations, and maintain standard methodologies for development of the Mapping Information Platform system. FEMA concurred with all of the findings and recommendations in our draft report, stating that our observations are valuable to its ongoing improvement efforts and that the recommendations are generally consistent with the agency's current plans. (OIG-05-44, September 2005, IT)

Security Weaknesses Increase Risks to Critical Emergency Preparedness and Response Database

We audited the DHS and its organizational components' security program to determine whether EP&R had implemented adequate and effective controls over sensitive data contained in its National Emergency Management Information System (NEMIS).

EP&R has not established adequate or effective database security controls for NEMIS. EP&R has developed and implemented many essential security controls for the NEMIS system, including the establishment of a change management process and the development of a NEMIS IT contingency plan. However, additional work remains to implement the access controls and continuity of operations safeguards necessary to protect sensitive NEMIS data adequately. EP&R has not (1) implemented effective procedures for granting, monitoring, and removing user access; or (2) conducted NEMIS IT contingency training or testing. In addition, vulnerabilities existed on NEMIS servers related to access rights and password administration, configuration management, as well as other security measures. We made several recommendations to assist EP&R to more effectively secure NEMIS.

In addition, to comply with the OMB's *Federal Information Security Management Act of 2002* (FISMA) reporting requirements, we evaluated the effectiveness of EP&R's information security program and practices as implemented for NEMIS. EP&R has not aligned fully its security program with DHS' overall policies, procedures, or practices. For example, security controls had not been tested in over a year; a contingency plan has not been tested; security control costs have not been integrated into the life cycle of the system; and, system and database administrators have not obtained specialized security training.

The EP&R CIO concurred with our recommendations and is in the process of implementing corrective measures. In addition, based on the results of our review, the CIO plans to implement an independent annual security assessment of NEMIS. (OIG-05-43, September 2005, IT)

Nine Individuals Arrested In Scheme To Obtain FEMA Funds after the World Trade Center Disaster
Nine individuals conspired and submitted fraudulent applications to FEMA stating that they lost their employment at a local barbershop due to the World Trade Center disaster on September 11, 2001. The owner of the barbershop provided signed letters to the individuals who submitted FEMA applications, certifying that they had lost their jobs at the barbershop due to 9/11 even though the barbershop was not affected by the disaster. All nine entered pleas of guilty and have been sentenced. (OI)

Fraudulent Hurricane Damage Applications (Update)
Our joint investigation with the U.S. Postal Inspection Service resulted in the arrest of 14 Miami-Dade County residents who were paid a total of more than $156,000 in disaster assistance for providing fraudulent information in their applications to FEMA. These individuals were charged with multiple counts of wire fraud, mail fraud and submitting false and fraudulent claims. Of the 14 subjects indicted, 13 pleaded guilty and one was acquitted at trial. (OI)

MANAGEMENT

Buy American Act Compliance
As directed by Congress in the FY 2005 Conference Report accompanying H.R. 4567, we audited DHS' compliance with the *Buy American Act (BAA) of 1933* (41 USC 10a-10d). We concluded that DHS and its organizational component procurement offices have sufficient policies and procedures to ensure compliance with BAA requirements. However, we were unable to fully validate compliance with BAA requirements because of DHS' inability to identify conclusively all procurements subject to BAA requirements and the tight time constraints under which the audit had to be conducted.

DHS organizational components have procurement oversight processes to ensure that Federal Acquisition Regulations (FAR) requirements, including BAA, are incorporated appropriately into contracts. In addition, neither the Federal Procurement Data System - Next Generation (FPDS-NG) nor the Homeland Security Contract Information System have the capability to collect data regarding the amounts and types of foreign end products being procured by DHS. While DHS organizational components identified acquisitions worth approximately $165 million involving foreign end products, these acquisitions do not represent the entire BAA universe at DHS. While DHS believes that acquisition of foreign end products occurs infrequently, system limitations make it difficult to determine the actual frequency of foreign acquisitions. Additionally, ICE incorrectly applied BAA evaluation factors during the source selection process for a major procurement of pistols. Finally, automated contract writing systems that help ensure BAA compliance are not available at all procurement offices at this time.

We recommended that the Office of the Chief Procurement Officer: 1) provide additional training to procurement personnel regarding the BAA requirements and the application and use of BAA evaluation factors; 2) complete the scheduled implementation of automated contract writing systems for all DHS organizational components to ensure compliance with BAA and other FAR requirements; 3) consult with OMB regarding the necessity for government-wide tracking of BAA compliance within FPDS-NG; 4) revise Homeland Security Contract Information System guidance to change the country of origin field to a mandatory field, when applicable; and 5) require organizational components to continue manual data collection on domestic and foreign end product data, until automated systems to collect this information become available. (OIG-05-23, June 2003, OA)

DHS' Efforts to Develop the Homeland Secure Data Network

Anticipating the need to share intelligence and other information securely to fulfill its homeland defense mission, DHS will streamline and merge disparate classified networks into a single, integrated network called the Homeland Secure Data Network (HSDN). Homeland security leaders envision that HSDN will become the major secure information thoroughfare joining together intelligence agencies, law enforcement, disaster management, and front-line disaster response organizations in the common goal of protecting our nation and its citizens.

DHS has taken a number of key steps toward the implementation of HSDN. These include establishing a Program Management Office for development and implementation of HSDN; performing tasks in the planning, requirements definition, and design phases of the DHS System Development Life Cycle process for the new network; defining the HSDN system concept; identifying some user requirements for HSDN; and, awarding a contract for the design, development, testing, and implementation of HSDN. Further, DHS used an appropriate approach for the acquisition of HSDN. DHS officials believed that the Department of Defense planned to terminate DHS' access to Defense's secure network, Secret Internet Protocol Router Network, by December 31, 2004. Accordingly, the DHS CIO established an aggressive nine-month timeframe to implement HSDN. However, this accelerated schedule prevented DHS from adequately completing critical system development requirements. Specifically, the methods for collecting and documenting the functional and security needs of users during the requirements definition phase for the new network did not provide adequate assurance that user needs at the 600 sites will be met. Further, security implementation requirements and essential testing had not been completed one month prior to deployment. Without completing and documenting these activities in sufficient time for review and adjustment to eliminate or mitigate risk, DHS does not have assurance that HSDN complies with security standards and policies.

We recommended that the CIO ensure that users are involved in the requirements definition process for all future implementation phases of HSDN, and verify that all necessary activities and documents, including certification and accreditation (C&A) and thorough security control testing, are completed prior to system deployment. (OIG-05-19, April 2005, IT)

Disaster Recovery Planning for DHS Information Systems Needs Improvement
Disaster recovery planning for information systems at 19 DHS facilities, and associated disaster recovery planning documentation, requires improvement. Specifically, 15 of the 19 (79%) facilities reviewed did not have a recovery site for their information systems - or the recovery site was not fully operational. While 4 of the 19 (21%) facilities had fully operational disaster recovery sites, tests at those facilities revealed deficiencies that could adversely impact recovery of critical information systems. Additionally, DHS disaster recovery planning documents, such as continuity of operations and contingency plans, need improvement. Deficiencies were identified in 25 of the 31 (81%) disaster recovery planning documents reviewed, and 13 of the 31 (42%) planning documents had not been finalized. These problems with disaster recovery are occurring in part because DHS does not have a program to provide an enterprise-wide disaster recovery solution.

DHS must be able to perform mission essential functions with minimal disruption following a service disruption or a disaster. The inability to restore DHS' critical information systems following a disaster, could have negative effects on DHS' performance. Potential effects could include a disruption in passenger screening operations, delays in processing grants in response to a disaster, or delays in the flow of goods across U.S. borders.

We made three recommendations to the DHS CIO: allocate the funds needed to implement an enterprise-wide disaster recovery program for mission critical systems; require that disaster recovery capabilities are included in the planning and implementation of new systems; and, require that disaster recovery-related documentation for mission critical systems be completed and conform to current government standards. The DHS CIO concurred with our findings and recommendations and has advised us on the actions that DHS will take to correct these deficiencies. (OIG-05-22, May 2005, IT)

DHS' Information Security Program for Fiscal Year 2005
To comply with OMB's FISMA reporting requirements, we evaluated DHS' information security program and practices. We focused our evaluation on whether DHS' major organizational components are aligning their information security program and practices with DHS' agency-wide information security program.

DHS achieved two significant milestones that will help the department move toward managing a successful information security program. First, DHS completed a comprehensive inventory of its major applications and general support systems, including contractor and national security systems, for all organizational components. Second, DHS implemented a department-wide C&A tool that incorporates the guidance required to adequately complete a C&A all systems. The completion of these two tasks eliminated two factors that significantly held the department back in achieving some success in establishing its security program in the last two years.

As we reported in our FY 2004 FISMA evaluation, and despite several major improvements in DHS' information security program, DHS organizational components, through their Information Systems Security Managers, have not completely aligned their respective information security programs with DHS' overall policies, procedures, and practices.

While DHS has issued substantial guidance designed to create and maintain secure systems, we identified areas where agency wide information security procedures require strengthening: (1) C&A; (2) vulnerability testing and remediation; (3) penetration testing; (4) contingency plan development and testing; (5) incident detection, analysis, and reporting; (6) security configuration; and, (7) specialized security training.

In our FY 2004 report, we identified issues to be addressed to assist DHS and its components in the implementation of its information security program. While some of these issues have been addressed, such as completing a comprehensive inventory; the majority of DHS' operational systems have not been certified and accredited. Further, POA&Ms have not been developed for all weaknesses. We recommend that DHS continue to consider its information security program a significant deficiency for FY 2005. DHS agreed with our recommendations. (OIG-05-46, September 2005, IT)

DHS' Security Program and Practices For Its Intelligence Systems

We conducted an evaluation of DHS' information assurance posture, including its policies and procedures, for the intelligence systems under its purview. We performed our work from May through July 2005. We focused our assessment on DHS' compliance with the *FISMA* for its intelligence systems in operation as of May 1, 2005, and containing Top Secret/Special Compartmented Information.

Overall, we identified issues with DHS' management structure for the department's intelligence systems. We also identified issues regarding DHS' inventory of its Special Compartmented Information systems, the C&A of its intelligence systems, plan of action and milestones (POA&M)s, incident detection and response, and information security training and awareness. DHS must address these issues in order to provide adequate security for the information and information systems that support intelligence operations

and assets and ensure the confidentiality, integrity, and availability of vital intelligence information. (OIG-05-34, August 2005, IT)

UNITED STATES COAST GUARD (USCG)

The Coast Guard's Civilian Pay Budget Process
In response to a request from the Chairman of the House Subcommittee on Homeland Security, Committee on Appropriations, we engaged the independent accounting firm KPMG LLP to perform an audit of USCG's FY 2004 civilian pay expenses and related budget reprogramming requests. KPMG reported that USCG had not designed appropriate processes and internal controls for the development and execution of the civilian pay budget. As a result, USCG had difficulty supporting its FY 2004 reprogramming requests with respect to civilian pay. Prior to FY 2004, civilian pay was part of a much larger budget category that included military pay. Thereafter, civilian pay became its own budget category, with more visibility. KPMG made several recommendations to improve USCG's budgeting process for civilian pay. (OIG-05-29, August 2005, OA)

Intelligence Oversight Quarterly Report
In accordance with Executive Order (EO) 12863, we submitted a Intelligence Oversight Quarterly Report of the USCG and the Office of Information Analysis (IA). Working closely with the Office of General Counsel, we continued to work on the directive implementing EO 12333 for IA, including U.S. personal information handling procedures, internal reporting and investigation processes, and general compliance with EO 12333 requirements. In addition to this effort, we conducted an informal inspection of the USCG Intelligence Coordination Center's (ICC) Intelligence Oversight program that affirmed that the ICC has a training program that provides effective initial and annual refresher intelligence oversight training to employees, has implemented safeguards in its operations to prevent violations of the rights of U.S. persons, and has established a systematic inspection plan to ensure adherence to EO 12333 and the USCG implementing documents. Random interviews of ICC personnel revealed that employees in each office were familiar with, and sensitive to, Intelligence Oversight issues, and knew whom to consult when they had questions about Intelligence Oversight.

Security Weaknesses Increase Risks to Critical United States Coast Guard Database
We audited the DHS and its organizational components' security program to determine the security and integrity of select sensitive but unclassified mission critical databases. Our audit included reviews of access controls, continuity of operations, and change management policies and procedures.

USCG has not established adequate or effective database security controls for its Marine Information for Safety and Law Enforcement (MISLE) system. USCG has developed and implemented many essential security controls for the MISLE system, including a process to control routine changes to the system and a process to maintain and review an audit trail of operating system level security events. USCG has not 1) implemented effective procedures for granting, monitoring, and removing user access; or 2) developed and tested an adequate IT contingency plan. In addition, vulnerabilities existed on MISLE servers related to access rights and password administration, configuration management, as well as other security measures. We made several recommendations to assist the USCG to more effectively secure MISLE.

In addition, to comply with the OMB's FISMA reporting requirements, we evaluated the effectiveness of USCG's information security program and practices as implemented for MISLE. USCG has not yet fully aligned its security program with DHS' overall policies, procedures, or practices.

USCG Chief of Staff concurred with our recommendations and is in the process of implementing corrective measures. In addition, POA&Ms will be created and tracked for the vulnerabilities we identified. (OIG-05-35, August 2005, IT)

Improved Security Required for U.S. Coast Guard Networks

We audited the DHS security program and its organizational components to determine the effectiveness of controls implemented on selected wired-based sensitive but unclassified networks. Our audit included a review of applicable DHS and USCG security policies, procedures, and other appropriate documentation. In addition, we performed vulnerability assessments to evaluate the effectiveness of controls implemented on selected network devices.

USCG relies on the Telecommunication and Information Systems Command for the overall management and security of its USCG Data Network Plus (CGDN+) network. However, different groups throughout the organization manage the LANs that connects to the CGDN+ network. For example, each major command, including USCG Headquarters, is responsible for managing its own LANs, configuring its own network devices, and deploying security patches.

USCG has not developed or implemented controls necessary to ensure that the data residing on and traveling through its network resources is properly protected. USCG has developed various policies, procedures, and processes to help monitor and secure its CGDN+ network and its LANs. However, USCG has not developed policies or procedures and fully implemented processes that address security testing, monitoring network activities with audit trails, and configuration and patch management. In addition, we noted that the CGDN+ network contingency plan has not yet been tested.

Security controls must be improved in order for USCG to provide adequate and effective security over its networks. Our vulnerability assessments identified security concerns resulting from inadequate password controls, missing critical patches, vulnerable network devices, and inconsistent configuration and patch management. These security concerns indicate increased potential for unauthorized access to USCG resources and data.

We made several recommendations to assist USCG to secure its networks. Effective network management and security controls are needed in order to protect the confidentiality, integrity, and availability of sensitive information. In response to our draft report, USCG agreed and has already taken steps to implement each of the recommendations. (OIG-05-30, August 2005, IT)

UNITED STATES SECRET SERVICE (USSS)

Improved Security Required for U.S. Secret Service Networks

We audited DHS and its organizational components' security program to determine the effectiveness of controls implemented on selected wired-based sensitive but unclassified networks. Our audit included a review of applicable DHS and USSS security policies, procedures, and other appropriate documentation. In addition, we performed vulnerability assessments to evaluate the effectiveness of controls implemented on selected network devices.

The USSS has not developed adequate policies or fully implemented procedures and processes that address security testing, monitoring network activities with audit trails, and configuration and patch management. Additionally, the USSS has not implemented the necessary controls to ensure that the data residing on and traveling through its network resources is properly protected.

Security controls must be improved in order for the USSS to provide adequate and effective security over its networks. Our vulnerability assessments identified security concerns resulting from inadequate password controls, missing critical patches, vulnerable network devices, and weaknesses in configuration management. Furthermore, our evaluation of router configuration determined that the USSS had not securely configured its routers to minimize unauthorized access to its networks. These security concerns provide increased potential for unauthorized access to USSS resources and data.

We made several recommendations to assist the USSS to secure its networks. Effective network management and security controls are needed to protect the confidentiality, integrity, and availability of sensitive information. The USSS agreed and has already

taken steps to implement each of the recommendations. (OIG-05-38, September 2005, IT)

Security Weaknesses Increase Risks to Critical United States Secret Service Database
We audited DHS and its organizational components' security program to determine the security and integrity of select sensitive but unclassified mission critical databases. Our audit included reviews of access controls, change management, and continuity of operations policies and procedures.

The USSS has not established adequate or effective database security controls for USSS Web (SSWeb). Although the USSS has developed and implemented many essential security controls—including a process to ensure that system access is removed upon employee separation as well as a change management policy for implementing routine and emergency changes—additional work remains to implement the access controls, configuration management procedures, and continuity of operations safeguards necessary to protect sensitive SSWeb data effectively. The USSS has not implemented effective procedures for user administration; established a configuration management plan; or, developed and tested an IT contingency plan. In addition, vulnerabilities existed on an SSWeb database server related to access rights and password administration, configuration management, as well as other security measures. We made several recommendations to assist the USSS to secure SSWeb.

In addition, to comply with the OMB's FISMA reporting requirements, we evaluated the effectiveness of the USSS's information security program and practices as implemented for SSWeb. The USSS has not yet fully aligned its security program with DHS' overall policies or procedures. For example, a contingency plan has not been established and tested; security control costs have not been integrated into the life cycle of the system; and, system and database administrators have not obtained specialized security training.

The USSS concurred with our recommendations and is in the process of implementing corrective measures. The USSS also advises that the recommendations we provided would be used to strengthen security on other component systems. (OIG-05-37, September 2005, IT)

UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES (USCIS)

USCIS Approval of H-1B Petitions Exceeded 65,000 Cap in Fiscal Year 2005
The Chairman of the Senate Finance Committee and the Chairman of the Subcommittee on Immigration, Border Security and Claims of the House Judiciary Committee,

requested that we review actions taken by USCIS officials regarding provision of H-1B non-immigrant status to more aliens in FY 2005 than was statutorily authorized.

We concluded that USCIS officials at all levels in Washington, D.C. and at the service centers were aware of and attempted to comply with the statutory limit on the number of persons granted H-1B status. However, USCIS had neither the technology nor an operational methodology to ensure compliance with the precise statutory ceiling. The USCIS "business process" of taking all petitions submitted before an announced cut-off date guarantees that an inexact number of petitions will be approved. Faced with the certainty of issuing either too few or too many approvals, it had been USCIS' explicit practice to avoid approving too few. We also determined that: the structure of DHS handicaps counting efforts; a complex adjudication process makes the count fluctuate; a complex counting process makes the cap a moving target; and, an unexpected influx of petitions in mid-September 2004 swamped the cap counting process.

Several recent USCIS initiatives are designed to prevent a recurrence. However, we believe that the new policies might not be sufficient to accomplish the precision that Congress now requires, and offered two recommendations to improve the methods for processing H-1B petitions. (OIG-05-49, September 2005, ISP)

Security Weaknesses Increase Risks to Critical United States Citizenship and Immigration Services Database

We audited USCIS' security program to determine whether USCIS had implemented adequate and effective controls over sensitive data contained in its Central Index System. Information contained in the Central Index System is used to assist in the enforcement of United States immigration laws.

Although USCIS has not established adequate or effective database security controls for the Central Index System, it has implemented many essential security controls such as procedures for controlling temporary or emergency system access, a configuration management plan, and procedures for implementing routine and emergency changes. Further, we did not identify any significant configuration weaknesses during our technical tests of the Central Index System. However, additional work remains to implement the access controls, configuration management procedures, and continuity of operations safeguards necessary to protect sensitive Central Index System data effectively. USCIS has not: 1) implemented effective user administration procedures; 2) ensured that system changes are properly controlled; 3) developed and tested an adequate IT contingency plan; or, 4) monitored system security functions sufficiently. We made several recommendations to assist USCIS to more effectively secure the Central Index System.

In addition, to comply with OMB's FISMA reporting requirements, we evaluated the effectiveness of the USCIS' information security program and practices as implemented for the Central Index System. USCIS has not aligned fully its security program with DHS' overall policies, procedures, or practices. For example, security controls are not routinely tested and evaluated; a contingency plan has not been established and tested; and, system and database administrators have not obtained specialized security training.

The USCIS acting deputy director concurred with our recommendations and is in the process of implementing corrective measures. In addition, USCIS is in the process of building an IT Security Office and implementing security, privacy, systems development, and continuity of operations best practices. (OIG-05-42, September 2005, IT)

USCIS Faces Challenges in Modernizing Information Technology

The effective use of IT is critical to increase efficiency and eliminate the backlog in immigration benefits processing. However, the USCIS faces the continuing challenge of overcoming longstanding operational and systems issues and modernizing its IT – even as it matures and evolves as a new bureau under the auspices of DHS. We conducted an audit to determine how well USCIS currently is managing IT, as well as to assess its IT modernization plans and its approach to implementing those plans across the organization.

We reported that USCIS' IT environment for processing immigration benefits continues to be inefficient, hindering its ability to carry out its mission. Specifically, USCIS' processes are primarily manual, paper-based, and duplicative, resulting in an ineffective use of human and financial resources to ship, store, and track immigration files. IT software and hardware systems also are not well configured to meet users needs, although USCIS recently has outlined plans to upgrade desktops and servers and consolidate data centers to help address these problems.

Further, despite federal requirements, USCIS has not had a focused approach to modernizing the processes and systems used to accomplish its citizenship and immigration services mission. IT planning and implementation typically has been conducted in a decentralized manner across the organization. In the interim, USCIS continues to rely on personnel rather than technology to meet its backlog reduction goals and other priorities. The bureau has not recognized the potential benefits of leveraging IT, streamlining processes, and coordinating improvement initiatives to better meet its mission objectives. The impact of the DHS reorganization, new security requirements, and changes to immigration legislation also pose challenges to effective modernization.

To help ensure more effective use of IT to support immigration benefits processing, we recommended that the acting deputy director develop a single strategy with performance measures for IT modernization, complete the implementation of plans to centralize IT,

and ensure that the centralized CIO operation and its IT transformation initiatives support the consolidated USCIS strategy. Also, USCIS must review, analyze, and reengineer benefits adjudication processes and finalize and implement plans to upgrade and standardize its IT hardware and software systems. Finally, USCIS must ensure representation and participation of users at the various levels from across USCIS in all process reengineering and IT transformation activities. The acting deputy director partially concurred with one recommendation and concurred with the remaining recommendations. The partial concurrence was based on obtaining the funding needed to implement the USCIS IT Transformation Program effectively. (OIG-05-41, September 2005, IT)

Improvements Needed In Security Management of the United States Citizenship and Immigration Services' CLAIMS 3 Mainframe Financial Application

The objective of our audit was to determine whether there is adequate management in place over the security of USCIS' CLAIMS 3 mainframe application. We concluded that access controls in place over the CLAIMS 3 mainframe are not sufficient to prevent unauthorized access to, or loss of, the system's immigration and customs information.

We recommended that the USCIS CIO:

- designate a USCIS CLAIMS 3 security administrator;
- develop and implement a set of policies and procedures for a coordinated effort of administering and managing the CLAIMS 3 mainframe security process between USCIS and ICE;
- establish procedures for a USCIS security administrator to review and monitor access controls security reports on a daily basis;
- establish procedures for a USCIS security administrator to re-certify user access privileges to the CLAIMS 3 mainframe at least on an annual basis;
- enforce DHS' remote access policy requiring that DHS systems be accessed only through DHS approved hardware and software;
- strengthen the CLAIMS 3 mainframe password configurations in accordance with DHS' Security Handbook; and,
- re-establish preventive maintenance and system upgrades for the CLAIMS 3 mainframe. (OIG-05-28, July 2005, IT)

Immigration Information Officer Admits to Selling Counterfeit Documents

On September 22, 2004, a USCIS immigration information officer was indicted on four counts of 18 USC §1546, Fraud and Misuse of Visas, Permits, and Other Documents. The officer had been creating and selling counterfeit INS "Notices of Approval" for employment authorization to undocumented Philippine aliens over a period of at least two years.

When confronted with the evidence developed during the investigation and the sound of his voice on recordings, he admitted to creating and selling counterfeit INS notices and labor certification documents as genuine documents to five known individuals. These documents were portrayed to authorize the buyers' employment and residence in the United States. He charged these individuals $6,000.

The officer pled guilty to the four counts of 18 USC §1546, Fraud and Misuse of Visas, Permits, and Other Documents on July 8, 2005. He is scheduled for sentencing on November 7, 2005. This case was investigated jointly with ICE Office of Professional Responsibility. (OI)

OTHER OIG ACTIVITIES

Oversight of Non-DHS OIG Audits
We processed 83 contract audits conducted by DCAA during the current reporting period. The DCAA reports questioned $16,336,559, of which $3,621,098 was unsupported. We continue to monitor the actions taken to implement the recommendations in the reports.

We also processed 100 single grant audit reports issued by other organizations. The single grant audit reports questioned $1,292,245, of which $522,544 was unsupported. The reports were conducted according to the Single Audit Act of 1984, as amended. 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 201 reports that contain recommendations that have been unresolved for more than six months. Management decisions have not been made for the following significant reports:

- Forty-four Single Audit Act reports

  Management is currently reviewing the reports and advises that it anticipates resolving the recommendations by March 31, 2006.

- Forty-seven grant audit reports

  Management is currently reviewing the reports and advises that it anticipates resolving the recommendations by March 31, 2006.

- Ten DCAA contract audit reports processed by the OIG

  Contracting officers are currently reviewing the reports and have advised that they anticipate resolving the recommendations by March 31, 2006.

- Twenty-three state disaster management contract audit reports

  Management is currently reviewing the reports and advises that it anticipates resolving the recommendations by March 31, 2006.

- The OIG continues to wait for a response from TSA that documents the actions it will take to address recommendations relating to screener training. The original action plan was due in January; a partial response in June lacked the specificity necessary to resolve 3 unresolved recommendations and to close 17 resolved but open recommendations.

LEGISLATIVE AND REGULATORY REVIEW

Section 4 (a) of the *IG Act* requires the IG to review existing as well as 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 the proposed legislation and regulations will have on the economy and efficiency in administering DHS programs and operations; or on the prevention and detection of fraud and abuse in DHS programs and operations. Additionally, 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.

We also review and comment on DHS management directives involving DHS programs and operations. During this reporting period, we reviewed 36 proposed DHS regulations and policy directives. Comments on three items are highlighted below:

Proposed Rulemaking for Staffing for Adequate Fire and Emergency Response Grant Program: We reviewed a draft proposed rule to provide potential applicants with guidance on a grant program that would provide federal funding for hiring new firefighters and retaining volunteer fire fighters. We recommended that the rule more clearly address program priorities and the basis upon which grants will be completed and awarded.

DHS Management Directive 0784 "Acquisition Oversight Program:" We recommended several changes to proposed policies and procedures for DHS acquisition oversight. Specifically, we recommended: (1) that proactive DHS acquisition oversight be conducted for major critical acquisitions to identify and solve problems before contract award; (2) improvements be made to a self-assessment questionnaire to be completed by DHS components and the questionnaire's data collection methods; (3) that identified significant deficiencies should be treated as more than "advisory" comments; and, (4) that oversight checklists be revised to better ensure that the quality of procurement file documentation is being assessed during the oversight process.

DHS Management Directive 11055 "Suitability Screening Requirements for Contractors:" This draft DHS guidance proposes suitability screening standards for contractor personnel. We recommended further clarification of the roles and responsibilities of departmental offices in implementing the directive and suggested more clearly defining the interrelationships of national security clearances and suitability determinations.

CONGRESSIONAL BRIEFINGS AND TESTIMONY

The Office was called upon to testify before Congress on eight occasions during this reporting period:

- Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, September 28, 2005 (Subject: *Post-Katrina Relief and Recovery: The Plans of the Inspectors General*)

- Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform, July 27, 2005 (Subject: *Financial Management at the Department*)

- Committee on Homeland Security and Governmental Affairs, U.S. Senate, May 18, 2005 (Subject: *FEMA's response to the 2004 hurricane season*)

- Committee on Commerce, Science, and Transportation, U.S. Senate, May 17, 2005 (Subject: *Port Security*)

- Subcommittee on Immigration, Border Security, and Claims, Committee on the Judiciary, U.S. House of Representatives, April 21, 2005 (Subject: *Visa Waiver Program and Biometric/Secure Passports*)

- Subcommittee on Management, Integration, and Oversight, Committee on Homeland Security, U.S. House of Representatives, April 20, 2005 (Subject: *DHS Management Challenges*)

- Subcommittee on Emergency Preparedness, Science, and Technology, Committee on Homeland Security, U.S. House of Representatives, April 12, 2005 (Subject: *First Responder Grant Programs*)

- Committee on Government Reform, U.S. House of Representatives, April 7, 2005 (Subject: *FISMA*)

Additionally, we met with members of Congress and their staff on a broad range of issues, including oversight of Hurricane Katrina and Rita spending, several investigative matters, compliance with the BAA, TSA non-screener administrative staffing issues, Philadelphia International Airport matter, ATS report, Tucson Sector checkpoints, DHS management issues, and secure data network and IT disaster recovery planning reports.

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]	123	$170,530,997	$63,245,950
B. Reports issued/processed during the reporting period with questioned costs [1]	31	$31,106,976	$8,118,945
Total Reports (A+B)	154	$201,637,973	$71,364,895
C. Reports for which a management decision was made during the reporting period	39	$31,933,938	$3,110,259
(1) Disallowed costs	35	$28,687,137	$2,473,280
(2) Accepted costs[2]	10	$1,753,781	$18,326
D. Reports put into appeal status during period	0	$0	$0
E. Reports pending a management decision at the end of the reporting period	115	$169,704,035	$68,254,636
F. Reports for which no management decision was made within six months of issuance	89	$154,833,990	$60,135,691

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] The questioned costs represent those costs reported by our Office and non-Federal auditors (i.e., DCAA and independent accounting firms for single grant audits).
[2] Single audit report #OIG-S-20-04 was processed in February 2004, reporting $46,916 in questioned, ineligible costs in error. The adjustment was included in Section C(2) above.

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.

In Category C, six (6) audit reports contained both allowed and disallowed costs.

Questioned costs – Auditors commonly question costs arising from an alleged violation of a provision of a law, regulation, grant, cooperative agreement or contract. A "questioned" cost is a finding in which, at the time of the audit, a cost 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 [1]	10	$60,340,936
B. Reports issued during this reporting period	0	$0
Total Reports (A + B)	10	$60,340,936
C. Reports for which a management decision was made during the reporting period[1]	2	$8,021,485
(1) Value of recommendations agreed to by Management	0	$0
(2) Value of recommendations not agreed to by Management [1 2]	2	$8,021,485
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	8	$52,319,451
F. Reports for which no management decision was made within six months of issuance	8	$52,319,451

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.

[1] Audit report #E-22-99 issued in March 1999 had associated $169,550 in Funds Put to Better Use (FPTBU). However, we have concluded that these funds are non-collectible. The adjustment was included in Section C(2) above.

[2] Audit report #OIG-00-111, a legacy audit report issued under the U.S. Department of Treasury in July 2000 had $7,960,444 in FPTBU that are uncollectible, based upon our management review. The adjustment was included in Section C(2) above.

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

4/1/2005	
Reports open over six months	136
Recommendations open over six months	565
9/30/05	
Reports open over six months	201
Recommendations open over six months	885

CURRENT INVENTORY

Open reports at the beginning of the period	325
Reports issued this period[1]	242
Reports closed this period	261
Open reports at the end of the period	306

ACTIVE RECOMMENDATIONS

Open recommendations at the beginning of the period	1,648
Recommendations issued this period	352
Recommendations closed this period	813
Open recommendations at the end of the period	1,187

Notes and Explanations:

[1]Includes 12 Management audit reports issued, 17 IT audit reports issued, 5 Inspection reports issued, 23 disaster grant audit reports issued, 83 DCAA audit reports processed, and 100 single audit reports processed. This number also includes two DCAA audit reports (OIG-C-03-05 and OIG-C-01-05) issued in March 2005, which were not previously reported. There were no questioned costs or audit recommendations associated with the two DCAA reports.

Appendix 3
Management Reports Issued

	Program Office/Report Subject	Report Number	Date Issued
1.	DHS' Efforts to Develop the Homeland Secure Data Network	OIG-05-19	4/05
2.	Audit of FEMA's Individuals and Households Program in Miami-Dade County, Florida, for Hurricane Frances	OIG-05-20	5/05
3.	Review of Controls Over the Export of Chemical and Biological Commodities	OIG-05-21	6/05
4.	Disaster Recovery Planning for DHS Information Systems Needs Improvement	OIG-05-22	5/05
5.	Audit of Buy American Act Compliance	OIG-05-23	6/05
6.	Letter Report: Immigration Enforcement Agent Position	OIG-05-24	6/05
7.	Letter Report: Citizenship Test Redesign	OIG-05-25	6/05
8.	Audit of Targeting Oceangoing Cargo Containers	OIG-05-26	7/05
9.	Information Technology Management Letter for the FY 2004 DHS Financial Statement Audit	OIG-05-27	7/05
10.	Improvements Needed in Security Management of the United States Citizenship and Immigration Services' CLAIMS 3 Mainframe Financial Application	OIG-05-28	7/05

Appendix 3
Management Reports Issued

	Program Office/Report Subject	Report Number	Date Issued
11.	The Coast Guard's Civilian Pay Budget Process	OIG-05-29	8/05
12.	Improved Security Required for U.S. Coast Guard Networks	OIG-05-30	8/05
13.	Improved Security Required for Transportation Security Administration Networks	OIG-05-31	8/05
14.	Audit of ICE's Budgetary Status and Other Areas of Concern	OIG-05-32	8/05
15.	Management Letter for the FY 2004 DHS Financial Statement Audit	OIG-05-33	8/05
16.	Evaluation of DHS' Security Program and Practices For Its Intelligence Systems	OIG-05-34	8/05
17.	Security Weaknesses Increase Risks to Critical United States Coast Guard Database	OIG-05-35	8/05
18.	Emergency Preparedness and Response Could Better Integrate Information Technology with Incident Response and Recovery	OIG-05-36	9/05
19.	Security Weaknesses Increase Risks to Critical United States Secret Service Database	OIG-05-37	9/05
20.	Improved Security Required for U.S. Secret Service Networks	OIG-05-38	9/05

Appendix 3
Management Reports Issued

	Program Office/Report Subject	Report Number	Date Issued
21.	Improved Security Required for U.S. Customs and Border Protection Networks	OIG-05-39	9/05
22.	Independent Auditor's Report on TSA's FY 2004 Financial Statements	OIG-05-40	9/05
23.	USCIS Faces Challenges in Modernizing Information Technology	OIG-05-41	9/05
24.	Security Weaknesses Increase Risks to Critical United States Citizenship and Immigration Services Database	OIG-05-42	9/05
25.	Security Weaknesses Increase Risks to Critical Emergency Preparedness and Response Database	OIG-05-43	9/05
26.	Challenges in FEMA's Flood Map Modernization Program	OIG-05-44	9/05
27.	A Review of DHS' Responsibilities for Juvenile Aliens	OIG-05-45	9/05
28.	Evaluation of DHS' Information Security Program for Fiscal Year 2005	OIG-05-46	9/05
29.	Vehicle Disposal and Sales Program Within U. S. Border Patrol's San Diego Sector	OIG-05-47	9/05
30.	National Flood Insurance Program Management Letter for DHS' Fiscal Year 2004 Financial Statement Audit	OIG-05-48	9/05

Appendix 3
Management Reports Issued

	Program Office/Report Subject	Report Number	Date Issued
31.	USCIS Approval of H-1B Petitions Exceeded 65,000 Cap in Fiscal Year 2005	OIG-05-49	9/05
32.	Review of the Immigration and Customs Enforcement's Compliance Enforcement Unit	OIG-05-50	9/05
33.	Transportation Security Administration Revised Security Procedures	OIG-05-51	9/05
34.	Transportation Security Administration's Procedures for Law Enforcement Officers Carrying Weapons On Board Commercial Aircraft	OIG-05-52	9/05

Appendix 4
Financial Assistance Audit Reports Issued

	Report Number	Date Issued	Auditee	Questioned Costs	Unsupported Costs	Funds Put to Better Use
1.	DA-15-05	4/05	Virgin Islands Department of Housing, Parks and Recreation	$0	$0	$0
2.	DA-16-05	5/05	City of Columbus, Mississippi	$192,578	$190,675	$0
3.	DA-17-05	6/05	Monroe County School District, Key West Florida	$411,026	$0	$0
4.	DA-18-05	6/05	City of Owensboro, Kentucky	$6,128	$0	$0
5.	DA-19-05	7/05	Lowndes County, Mississippi	$0	$0	$0
6.	DA-20-05	7/05	Audit of the State of Pennsylvania, Administration of Disaster Assistance Funds	$0	$0	$0
7.	DA-21-05	7/05	Audit of the District of Columbia Administration of Disaster Assistance Funds	$0	$0	$0
8.	DA-22-05	8/05	Municipality of Coamo, Puerto Rico	$928,048	$445,149	$0
9.	DA-23-05	8/05	City of Portsmouth, Virginia	$34,864	$0	$0
10.	DA-24-05	8/05	City of Clarksville, Tennessee	$22,947	$0	$0
11.	DA-25-05	8/05	Audit of the State of Florida Administration of Disaster Assistance Funds	$597,855	$0	$0

Appendix 4
Financial Assistance Audit Reports Issued

	Report Number	Date Issued	Auditee	Questioned Costs	Unsupported Costs	Funds Put to Better Use
12.	DA-26-05	8/05	Audit of the State of New Hampshire Administration of Disaster Assistance Funds	$0	$0	$0
13.	DA-27-05	8/05	Audit of the State of Vermont Administration of Disaster Assistance Funds	$0	$0	$0
14.	DA-28-05	9/05	Audit of First Responder Grant Funds Awarded to the Virgin Islands Law Enforcement Planning Commission	$111,540	$0	$0
15.	DD-05-05	4/05	Columbia Space Shuttle Mission Assignment National Forests and Grasslands in Texas, Lufkin, Texas	$3,415,340	$1,488,573	$0
16.	DD-06-05	5/05	Central Rural Electric Cooperative, Inc. Stillwater, Oklahoma	$1,406,493	$0	$0
17.	DD-07-05	6/05	Management Issues Identified During the Audit of Texas' Compliance With Disaster Assistance Program's Requirements	$0	$0	$0
18.	DD-08-05	7/05	Kiamichi Electric Cooperative, Inc. Wilburton, Oklahoma	$5,657,548	$1,648,454	$0
19.	DD-09-05	9/05	Western Farmers Electric Cooperative Anadarko, Oklahoma	$245,901	$4,290	$0

Appendix 4
Financial Assistance Audit Reports Issued

	Report Number	Date Issued	Auditee	Questioned Costs	Unsupported Costs	Funds Put to Better Use
20.	DS-13-05	7/05	Audit of the City of San Jose, California	$262,285	$198,162	$0
21.	DS-14-05	8/05	Audit of Kern County, California, Bakersfield, California	$0	$0	$0
22.	DS-15-05	8/05	Audit of the Ventura County Flood Control District Ventura, California	$0	$0	0
23.	DS-16-05	9/05	City of Santa Clarita	$149,319	$0	$0
24.	OIG-05-20	5/05	Audit of FEMA's Individuals and Households Program in Miami-Dade County, Florida, for Hurricane Frances[1]	$36,300	$0	$0
			Subtotal Disaster Audits	**$13,478,172**	**$3,975,303**	**$0**
25.	OIG-S-32-05	4/05	State of Nebraska	$514,676	$514,676	$0
26.	OIG-S-33-05	4/05	City of Pleasantville, New Jersey	$2,186	$0	$0
27.	OIG-S-58-05	6/05	City of Murfreesboro, Tennessee	$6,743	$6,743	$0
28.	OIG-S-99-05	7/05	State of Alabama	$1,125	$1,125	$0
29.	OIG-S-107-05	7/05	National Association of State Fire Marshals of Albany, New York	$1,385	$0	$0
30.	OIG-S-121-05	8/05	Government of Guam	$318,393	$0	$0

Appendix 4
Financial Assistance Audit Reports Issued

	Report Number	Date Issued	Auditee	Questioned Costs	Unsupported Costs	Funds Put to Better Use
31.	OIG-S-123-05	8/05	State of South Carolina	$447,737	$0	$0
			Subtotal Single Audits	**$1,292,245**	**$522,544**	**$0**
32.	OIG-C-08-05	4/05	Report on Audit of Parts of a Firm-Fixed Price Proposal for Field Service Representative Services: Dassault Falcon Jet Corporation	$83,099	$0	$0
33.	OIG-C-11-05	4/05	Audit Report on Proposal No. 04-R-00003: Yarrow Associates	$1,601,333	$0	$0
34.	OIG-C-13-05	5/05	Audit of Delay/Disruption Price Adjustment Claim: Water Pollution Control, Inc.	$377,313	$0	$0
35.	OIG-C-14-05	5/05	Report on the Agreed-Upon Procedures for Baggage Screen Proposal: Jackson Hole Airport Board	$24,102	$0	$0
36.	OIG-C-16-05	8/05	Report on Audit of Parts of a Firm-Fixed Price Proposal for Sustaining Engineering Services: Dassault Falco Jet Corporation	$46,980	$0	$0
37.	OIG-C-29-05	8/05	Supplemental Audit of Parts of a Proposal Submitted in Response to Request for Proposal No. HSTS03-04-COO032	$9,513	$0	$0

Appendix 4
Financial Assistance Audit Reports Issued

	Report Number	Date Issued	Auditee	Questioned Costs	Unsupported Costs	Funds Put to Better Use
38.	OIG-C-33-05	8/05	Audit Report of Contract Line Item Numbers 001 and 005 Quantum Under Department of Transportation Board of Contract Appeals Docket Number 4049: Macsons, Inc.	$60,582	$0	$0
39.	OIG-C-34-05	8/05	Audit Report on the Core Program Management CLIN Proposal: Unisys Corporation US Federal Government Group	$11,806,204	$3,621,098	$0
40.	OIG-C-45-05	8/05	Audit Report on Evaluation of Equitable Adjustment Claims: JHM Research & Development, Inc.	$2,327,433	$0	$0
			Subtotal DCAA Audits[2]	**$16,336,559**	**$3,621,098**	**$0**
			TOTAL	**$31,106,976**	**$8,118,945**	**$0**

Note: The narrative identifies 100% 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 have to calculate.

[1]This is a program management report with questioned costs.
[2]Of the 100 single audits processed and 83 DCAA audits processed during the period, the Appendix lists only those Single Audits and DCAA audits that had questioned costs.

Report Number Acronyms:
DA Disaster, Atlanta
DD Disaster, Dallas
DS Disaster, San Francisco
OIG-C DCAA Audits
OIG-S Single Audits

Appendix 5
Schedule of Amounts Due and Recovered

	Report Number	Date Issued	Auditee	Amount Due	Recovered Costs
1.	DA-30-03	9/03	Baltimore County, Maryland		$39,801
2.	DO-18-03	8/03	Simi Valley Unified School District City of Simi Valley California		$2,164,299
3.	DD-12-04	8/04	Audit of Hempstead County, Arkansas		$749,896
4.	DS-22-04	9/04	Audit of the County of Yuba, Marysville, California		$49,828
5.	A-S-14-04	1/04	City of Thibodaux, Louisiana		$16,653
6.	OIG-S-33-05	4/05	City of Pleasantville, New Jersey		$1,171
7.	DA-21-04	3/04	Municipality of Ceiba		$434,707
8.	DA-13-04	2/04	Virgin Islands Department of Public Works		$733,016
9.	DA-08-04	1/04	Municipality of Rio Grande		$347,689
10.	DS-04-05	12/04	Audit of the City of Pacifica, California		$25,769
11.	DS-03-05	1/04	Audit of Humboldt County, Eureka, California		$18,296
12.	DS-05-05	12/04	Audit of Daly City, California		$53,678
13.	DS-07-05	1/05	Audit of Glenn County, Willows, California		$85,997

Appendix 5
Schedule of Amounts Due and Recovered

	Report Number	Date Issued	Auditee	Amount Due	Recovered Costs
14.	DA-07-05	12/04	Jackson Energy Cooperative Corporation		$85,649
15.	DA-13-05	3/05	Pitt County, North Carolina		$296,318
16.	DA-04-05	10/04	Edgecombe County, North Carolina		$15,611
17.	DS-06-05	12/04	County of Ventura, Ventura, California		$89,369
18.	DS-08-05	2/05	Santa Monica Hospital Medical Center		$1,426,109
19.	DS-10-05	3/05	Public Assistance Grant Funds Advanced to the City of Los Angeles, Department of General Services		$512,381
20.	DS-11-05	3/05	City of Los Angeles, Department of Building and Safety, Los Angeles, California		$1,934,808
21.	DS-05-04	1/04	Newhall County Water District, Santa Clarita, California		$1,460,255
22.	DS-07-04	2/04	Santa Barbara County, Santa Barbara, California		$276,508
23.	DO-09-03	5/03	Kaiser Foundation Hospital, Los Angeles, California		$166,019
24.	DS-12-04	5/04	Santa Clarita Health Care Association, Santa Clarita, California		$1,893,976

Appendix 5
Schedule of Amounts Due and Recovered

	Report Number	Date Issued	Auditee	Amount Due	Recovered Costs
25.	DS-18-04	8/04	Conejo Valley United School District, Thousand Oaks, California		$39,740
26.	DS-20-04	9/04	Los Angeles Housing Authority, Los Angeles, California		$620,687
27.	OIG-S-107-05	7/05	National Association of State Fire Marshals of Albany, New York		$1,385
28.	DS-02-05	11/04	County of Monterey, Salinas, California		$96,803
			TOTAL	**$0**	**$13,636,418**

Appendix 6
Acronyms

ATS	Automated Targeting System
BAA	Buy America Act
BPA	Border Patrol Agent
C&A	Certification and Accreditation
CBP	Customs and Border Protection
CEU	Compliance Enforcement Unit
CGDN+	USCG Data Network Plus
CIO	Chief Information Officer
CREC	Central Rural Electric Cooperative
DCAA	Defense Contract Audit Agency
DHS	Department of Homeland Security
DRO	Detention and Removal Operations
EO	Executive Order
EP&R	Emergency Preparedness and Response
FAMS	Federal Air Marshal Service
FAR	Federal Acquisition Regulations
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Management Act of 2002
FOUO	For Official Use Only
FPS	Federal Protective Service
FY	Fiscal Year
IA	Information Analysis
ICC	Intelligence Coordination Center
ICE	United States Immigration and Customs Enforcement
IEA	Immigration Enforcement Agents
IG	Inspector General
IHP	Individuals and Households Program
INS	Immigration and Naturalization Service
ISP	Office of Inspections, Evaluations, and Special Reports
IT	Information Technology
LAN	Local Area Network
MISLE	Marine Information for Safety and Law Enforcement
NEMIS	National Emergency Management Information System
NFIP	National Flood Insurance Program
OA	Office of Audits
ODCEM	Oklahoma Department of Civil Emergency Management
OI	Office of Investigations

Appendix 6
Acronyms

OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
TSA	Transportation Security Administration
TS/SCI	Top Secret/Special Compartmented Information
USC	United States Code
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Services
USSS	United States Secret Service
US-VISIT	United States Visitor and Immigrant Status Indicator Technology
WAN	Wide Area Network
WFEC	Western Farmers Electric Cooperative

Appendix 7
OIG Headquarters and Field Office Contacts

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**
Richard Berman	**……...**	**Assistant Inspector General/Audits**
Elizabeth Redman	**……...**	**Assistant Inspector General/Investigations**
Robert Ashbaugh	**……...**	**Assistant Inspector General/Inspections**
Frank Deffer	**……...**	**Assistant Inspector General/Information Technology**
Edward F. Cincinnati	**……...**	**Assistant Inspector General/Administration**
Matt Jadacki [1]	**……...**	**Assistant Inspector General/Hurricane Katrina Oversight**
Tamara Faulkner	**……...**	**Congressional Liaison and Media Affairs**
Denise S. Johnson	**……...**	**Executive Assistant to the Inspector General**

[1] On detail from the Department of Commerce

Locations of Audit Field Offices

Atlanta, GA
3003 Chamblee-Tucker Rd., Suite 374
Atlanta, GA 30341
(770) 220-5228 / Fax (770) 220-5259

Boston, MA
10 Causway 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 350
Miramar, FL 33027
(954) 602-1980 / Fax (954) 602-1033

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

San Francisco, CA
300 Frank H. Ogawa Plaza, Suite 275
Oakland, CA 94612
(510) 627-7007 / Fax (510) 627-7017

St. Thomas, VI
Nisky Center, Suite 210
St. Thomas, VI 00802
(340) 774-0190 / Fax (340) 774-0191

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

Locations of Investigative Field Offices

Atlanta, GA
3003 Chamblee - Tucker Rd., Suite 301
Atlanta, GA 30341
(770) 220-5290 / Fax (770) 220-5288

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

Buffalo, NY
138 Delaware Ave., Suite 524
Buffalo, NY 14202
(716) 843-5700 x520 / Fax (716) 551-5563

Chicago, IL
55 W. Monroe St., Suite 1010
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
Levin Federal Courthouse
231 W. Lafayette, Suite 1044
Detroit, MI 48226
(313) 226-2163 / Fax (313) 226-6405

El Centro, CA
321 South Waterman Ave., Suite 108
El Centro, CA 92243
(760) 335-3549 / Fax (760) 335-3534

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

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 78041
(956) 794-2917 / 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) 618-8145 / Fax (956) 618-8151

Miami, FL
3401 SW 160th Ave., Suite 401
Miramar, FL 33027
(954) 602-1980 / Fax (954) 602-1033

Locations of Investigative Field Offices

New York City, NY
525 Washington Blvd., Suite 2407
Jersey City, NJ 07310
(201) 798-8165 / Fax (201) 659-5911

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

Seattle, WA
Carillon Point 2000
2360 Carillon Point, Suite 2360
Kirkland, WA 98033
(425) 576-4192 / Fax (425) 576-4191

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

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

Tucson, AZ
2120 West Ida Rd., Suite 286
Tucson, AZ 85701
(520) 670-5243 / Fax (520) 670-5246

Washington, DC
(Washington Field Office)
1300 North 17th St., Suite 526
Arlington, VA 22209
(703) 235-0848 / Fax (703) 235-0854

Yuma, AZ agents are temporarily operating out of the El Centro, CA field office.

Locations of Hurricane Katrina Oversight Field Offices

Austin, TX
Northview Business Center
9001 North I-35
Austin, TX 78753
(512) 977-4185 / Fax (512) 977-4640

Baton Rouge, LA
FEMA JFO/DR 1603-LA
415 N. 15th Street
Baton Rouge, LA 70802
(225) 242-6158 / Fax (225) 379-4020

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

Montgomery, AL
1555 Eastern Boulevard
Montgomery, Al 36117
(334) 409-4634

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	39-40
Significant Problems, Abuses, and Deficiencies	5-38
Recommendations with Significant Problems	5-38
Prior Recommendations Not Yet Implemented	38-39
Matters Referred to Prosecutive Authorities	1
Summary of Instances Where Information Was Refused	N/A
Listing of Audit Reports	48-56
Summary of Significant Audits	5-38
Reports with Questioned Costs	43-44; 52-56
Reports Recommending That Funds Be Put To Better Use	45-46
Summary of Reports in Which No Management Decision Was Made	38-39; 43-46
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.