DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

SEMIANNUAL REPORT TO THE CONGRESS

April 1, 2004 - September 30, 2004

Statistical Highlights of OIG Activities

April 1, 2004 - September 30, 2004

Dollar Impact

Questioned Costs	$23,497,249
Funds Put to Better Use	$0
Management Agreement That Funds Be:	
Recovered	$0
De-obligated	$0
Funds Recovered (Investigative Recoveries)	$0
Funds Recovered (Audit Recoveries)	$3,180,639
Fines and Restitutions	$1,300,762
Administrative Cost Savings and Recoveries	$0

Activities

OIG Reports Issued (Audits and Inspections)	63
OIG Reports Issued (Investigations)	220
Contract Reports Processed	0
Single Audit Reports Processed	21
Defense Contract Audit Agency	18
Investigations Initiated	1,074
Investigations Closed	235
Open Investigations	874
Investigations Referred for Prosecution	96
Investigations Accepted for Prosecution	28
Investigations Declined for Prosecution	36
Arrests	112
Indictments	105
Convictions	58
Personnel Actions	7
Total Complaints Received	4,209
Total Hotlines Received	838
Complaints Referred (to programs or other agencies)	3,895
Complaints Closed	3,795

Office of Inspector General

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

Homeland Security

November 1, 2004

The Honorable Tom Ridge
Secretary
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Mr. Secretary:

Enclosed herewith is our fourth semiannual report to the Congress since the establishment of the Department of Homeland Security (DHS) and the Office of Inspector General (OIG) in January, 2003. This report covers the period ended September 30, 2004. Per Section 5(b) of the Inspector General Act of 1978, as amended, please transmit this report, along with any comments, to the appropriate congressional committees and subcommittees no later than thirty days from today.

Of particular note in this period's compilation are several reports that relate to security vulnerabilities that can be exploited by terrorists. In particular, I call your attention to our reports on: (1) the undercover tests our auditors conducted at 15 airports throughout the country to determine whether threat items can evade detection by airport screeners; (2) the efficacy of the Visa Security Officer program in Saudi Arabia; (3) the visa waiver program and the problem of lost and stolen passports; (4) the status of efforts to consolidate terrorist watch lists; and (5) cargo security and uranium smuggling. It is critical that our recommendations in these reports be carried out as thoroughly and expeditiously as possible so as to assure the American people that the department is doing everything within its power to keep the nation safe.

It is also worthy of note that there has been progress in our long running effort to ensure that DHS employees are aware of their legal right to refer allegations of wrongdoing directly to OIG for investigation and that the department's internal affairs units promptly refer to OIG allegations that are within our jurisdictional purview. We are grateful to the Deputy Secretary for issuing a management directive on this subject that had been stalled in the clearance process for nearly a year. Significantly, that directive gives employees the option of reporting allegations to either OIG or an internal affairs unit, and it incorporates and institutionalizes the memoranda of understanding we had reached with such units requiring them promptly to refer criminal and serious non-criminal allegations

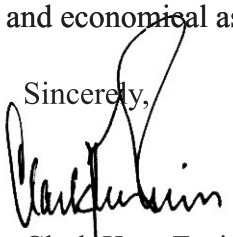
to OIG for our investigative consideration before they begin any investigative work of their own. Perhaps as a consequence of the issuance of this directive, internal affairs units are generally cooperating with OIG by referring matters to our attention that should be so referred.

That said, we are aware of at least two occasions when, for no exigent reason, significant investigative activity was undertaken before advising OIG and obtaining our consent. In one case, that of a Chinese national who was allegedly assaulted by a border inspector, interviews were taken and a prosecutorial referral was made hours before OIG was contacted.

And, I renew my request that you or another senior management official disseminate the management directive to all employees under your signature, so that we can be assured that all employees are advised of their rights and responsibilities thereunder and that management expects employees to exercise those rights and to discharge those responsibilities. While the directive is on the department's website along with others, it is doubtful that most employees make a practice of consulting the website regularly for directives that might be applicable to them. Employees cannot avail themselves of rights that they are not aware of, and OIG cannot investigate allegations that we are not aware of.

As always, we look forward to continuing to work with you and your leadership team to make the department as effective, efficient, and economical as it can be.

Sincerely,



Clark Kent Ervin
Inspector General

Table of Contents

Letter to the Secretary…….. i

Executive Summary…… 1

Department of Homeland Security Profile…….. 3

Office of Inspector General Profile……. 4

Summary of Significant OIG Activity by DHS Directorate or Component
- Border and Transportation Security……. 5
- Information Analysis and Infrastructure Protection…… 31
- Emergency Preparedness and Response…….. 33
- Management…….. 43
- United States Coast Guard...……..……. 48

Other OIG Activities
- Oversight of Non-DHS Audits…… 55
- Significant Audit Reports Unresolved Over Six Months……...… 56

Legislative and Regulatory Review……. 56

Congressional Briefings and Testimony…….. 57

Appendices

Appendix 1……. Audit Reports with Questioned Costs…….. 62
Appendix 1b….. Audit Reports with Funds Be Put to Better Use…..…… 63
Appendix 2……. Compliance - Resolution of Reports and Recommendations….. 64
Appendix 3……. Management Reports Issued…… 65
Appendix 4……. Financial Assistance Audit Reports Issued…..…… 67
Appendix 5……. Schedule of Amounts Due and Recovered…...…… 69
Appendix 6……. Acronyms……. 71
Appendix 7……. OIG Headquarters and Field Office Contacts and Locations….. 73
Appendix 8……. Index to Reporting Requirements……. 77

Executive Summary

This is the fourth Semiannual Report to the Congress issued by the Department of Homeland Security's (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, 2004 to September 30, 2004, unless otherwise noted. The report is organized to reflect the organization of the department and OIG.

During this reporting period, the OIG completed significant audit, inspection, and investigative work to promote the economy, efficiency, effectiveness and integrity of DHS programs and operations. Specifically, the OIG issued 26 audit, inspections, and information technology reports (Appendix 3). The OIG also issued 220 investigative reports. Additionally, the OIG issued 37 financial assistance audit reports (Appendix 4) and processed 39 reports on DHS programs—18 contract audits issued by DCAA, and 21 grant audits issued by other organizations in accordance with OMB Circular A-133.

The OIG supported the departmental effort to secure the homeland and make the American people safer by producing the following particularly noteworthy reports: Audit of Passenger and Baggage Screening Procedures at Domestic Airports (OIG-04-037 Issued September 2004); DHS Challenges in Consolidating Terrorist Watch List Information (OIG-04-031 Issued August 2004); Evaluation of the Federal Air Marshal Service (OIG-04-032 Issued August 2004); A Review of the Use of Alternative Screening Procedures at an Unnamed Airport (OIG-04-028 Issued July 2004); Effectiveness of Customs and Border Protection's Procedures to Detect Uranium in Two Smuggling Incidents (OIG-04-040 Issued September 2004); Review of the TSA Passenger and Baggage Screening Pilot Program (OIG-04-047 Issued September 2004); Review of TSA Screening Practices in Houston, Texas (OIG-04-048 Issued September 2004); and An Evaluation of the Security Implications of the Visa Waiver Program (OIG-04-026 Issued April 2004). The OIG reports provide the Secretary and the Congress with an objective assessment of the issues, while also providing specific recommendations to correct deficiencies, improve the efficiency, effectiveness and economy of the respective program, and make the American people safer.

During the reporting period, the OIG's audits, inspections, and investigations resulted in questioned costs of $23,497,249 (of which $4,165,518 were determined to be unsupported costs). Additionally, recoveries, restitutions, and fines totaled $4,481,401. The OIG's investigations resulted in 112 arrests, 105 indictments and 58 convictions. In

addition, investigators closed 235 investigations and 3,795 complaints received through the hotline.

The OIG has a dual reporting responsibility, to the Congress as well as to the Secretary. During the reporting period, the OIG continued its active engagement with Congress through numerous meetings, briefings, and dialogue with members and staff of the department's authorizing and appropriations committees and subcommittees on a range of issues relating to the work of the OIG and DHS. The Inspector General (IG) testified before Congress four times during this reporting period. On April 22, the IG testified before the House Committee on Transportation and Infrastructure, Subcommittee on Aviation, on the Airport Screener Privatization Pilot Program. On June 23, the IG testified before the House International Relations Committee on stolen passports and the findings reported in the OIG report, "An Evaluation of the Security Applications of the Visa Waiver Program." Then, on July 8, the IG testified before the Senate Governmental Affairs' Subcommittee on Financial Management, the Budget, and International Security, on the consolidated financial statements of the departments of Defense and Homeland Security. Finally, on September 9, 2004, the IG testified before the House Government Reform Committee on the cooperation between the Departments of State and Homeland Security on issues affecting U.S. visa policy, and discussed the findings of the following two OIG reports: *An Evaluation of DHS Activities to Implement Section 428 of the Homeland Security Act of 2002*, concerning the assignment of DHS personnel called "Visa Security Officers" (VSOs) to Saudi Arabia initially, and eventually to other countries around the world; and the April 2004 report, *An Evaluation of the Security Implications of the Visa Waiver Program,* concerning the security implications of the visa waiver program. Brief summaries of these four hearings are included in the "Congressional Briefings and Testimony" section of this report.

Department of Homeland Security Profile

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

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

The department has been organized into the following five directorates:

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

Other critical components of DHS include the:

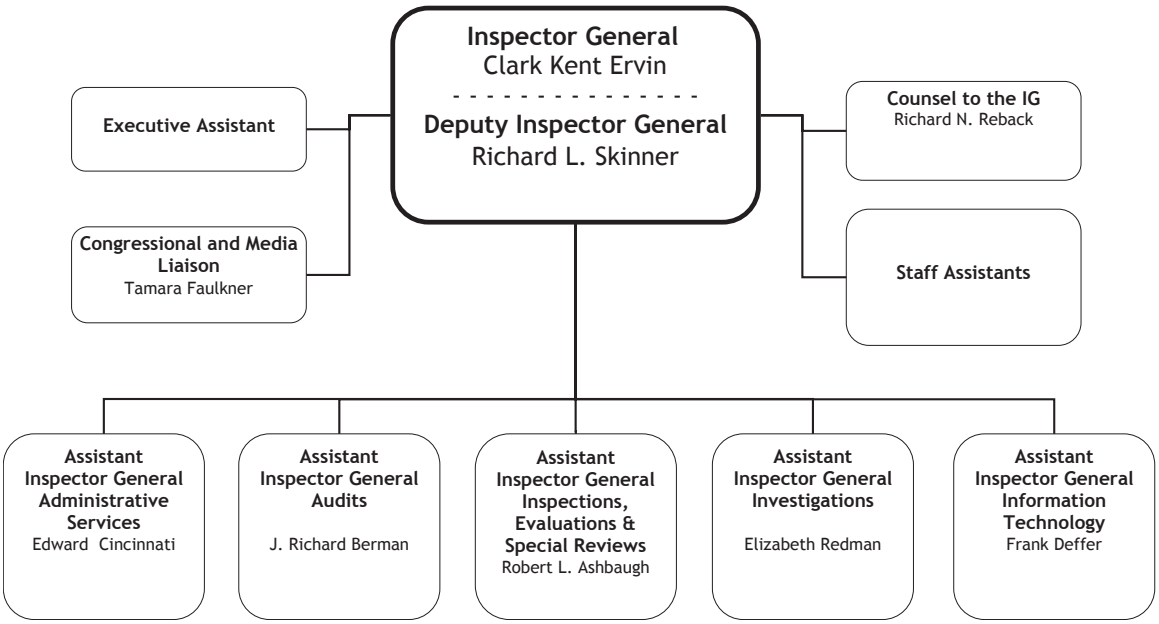
- United States Coast Guard
- United States Secret Service

Office of Inspector General Profile

The Homeland Security Act of 2002 provided for the establishment of an OIG in DHS by amendment to the Inspector General Act of 1978 (Public Law 95-452, as amended). By this action, Congress and the administration ensured independent and objective audits, inspections, and investigations of the operations of the department.

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

The OIG, which is authorized to have 502 full-time employees, is comprised of five functional components and is based in the District of Columbia. The OIG currently has 26 field offices throughout the country.



Summary of Significant OIG Activity by DHS Directorate or Component

Border and Transportation Security (BTS)

An Evaluation of DHS Activities to Implement Section 428 of the Homeland Security Act of 2002

Section 428 of the Homeland Security Act of 2002 authorizes BTS to review visa applications submitted at U.S. embassies and consular posts abroad. This includes the assignment of Visa Security Officers (VSO) to the embassies and consulates and the development of related program activities. While BTS has made progress in meeting Section 428 requirements, OIG's Office of Inspections, Evaluations, and Special Reviews (ISP) found that BTS has not complied with all requirements. For example, BTS was slow to assign VSOs to Saudi Arabia as required under the law. Further, BTS has not developed a plan to provide homeland security training to Department of State consular officers or plans to train VSOs in foreign languages, interview and fraud detection techniques, or foreign country conditions. BTS has not developed the required performance standards to evaluate consular officers. Finally, at the time of the OIG's review, BTS had not specified the criteria to select other consular posts for assigning VSOs or submitted the associated required reports to Congress.

The OIG's review of BTS' VSO operations in Saudi Arabia identified specific problems with program operations. Most of the VSOs who served in Saudi Arabia could not read or speak Arabic. This places severe limitations on their effectiveness and reduces their contribution to the security of the visa process. In addition, VSOs do not have adequate administrative support because BTS does not have a funding plan for VSO operations. At the time of the OIG's review, VSOs spent much of their time entering data to conduct database searches because DHS and State Department databases and information systems were not inter-connected. BTS and other law enforcement and intelligence agencies have not reviewed thousands of visa applications submitted and approved during the two years prior to the September 11th attacks for possible connection to terrorism. (OIG-04-033, August 2004, ISP)[1]

[1] The abbreviations, ISP, OA, IT, and OI, stand for the OIG component, Inspections, Audits, Information Technology, or Investigations, respectively, responsible for producing a given report.

An Evaluation of the Security Implications of the Visa Waiver Program

The Visa Waiver Program (VWP) enables citizens of 27 countries to travel to the United States for tourism or business for 90 days or less without obtaining a visa. The OIG identified significant areas where BTS needs to strengthen and improve VWP performance. Since the dissolution of the Immigration and Naturalization Service (INS), the VWP has had a series of acting managers and responsibility for the program has been diffused among DHS components. At the time of the OIG's review, responsibility for the VWP program was not clear to many within DHS or other federal agencies. This ambiguity, coupled with funding issues, threatened to render BTS delinquent in its conduct of mandatory country reviews of each VWP-designated country every two years. In addition, lost and stolen passports (LASP) constitute VWP's most serious security problem. BTS has not thoroughly checked LASP against U.S. entry and exit information to determine whether the passports have been used to enter the United States. Collection of LASP data from VWP governments is not proactive or uniform, nor is the data disseminated in an organized fashion. Further, LASP problems are complicated by the lack of international standardization in passport numbering systems that can result in a failure to identify male fide travelers using stolen VWP passports. In addition to corrective action responsive to the above issues, the OIG recommended that VWP passports be subjected to processing under United States Visitor and Immigrant Status Indicator Technology (US-VISIT) procedures, and that passport fraud training for inspectors at ports of entry be improved. (OIG-04-026, April 2004, ISP)

Transportation Security Administration (TSA)

Evaluation of the Transportation Security Administration's Screener Training and Methods of Testing

Steps taken by the TSA to update, modify, and improve the training and testing of security screeners incrementally improved basic screener training. TSA's December 2003 revisions to the passenger and checked baggage basic training aligned the course materials with TSA's latest standard operating procedures, presented detailed and technically accurate information, and addressed many instructional topics in sufficient depth. Furthermore, TSA revised and eliminated repetitive and simplistic test questions that the OIG noted during a previous review (ISP-02-03, August 2003). The curriculum and test revisions, however, were not supported by a systematic or comprehensive instructional systems design process and, as a result, were incomplete. Classroom and on-the-job training could have benefited from more thorough advance planning and analysis to select course content and frame the curriculum. Test design and administration for the basic classroom and on-the-job-training require greater standardization and validation.

TSA needs to train screeners in the classroom on the models of equipment they will be using on the job. Based on internal analyses, TSA began to incorporate some of these revisions in its April 2004 version of basic screener training. For recurrent training, TSA made significant improvements, setting a three-hour-per-week screener training requirement and distributing an array of training materials and tools to airports. TSA also recently completed its first annual screener re-certification testing. However, to maximize their benefit, both programs require further development. The OIG made 22 recommendations to the TSA Administrator to improve security screener training and methods of testing. (OIG-04-045, September 2004, ISP)

Assessment of Expenditures Related to the First Annual Transportation Security Administration Awards Program and Executive Performance Awards

TSA spent approximately $461,745 to host the First Annual TSA Awards program. In the OIG's view, many of the expenditures associated with the program were too high. Because the initial estimate for the awards ceremony site was less than $100,000, TSA was not required to solicit competitive bids when selecting a site for the awards program and did not compare the total costs associated with different sites and ceremony configurations. Although not required, it would have been a good business practice for TSA to solicit competitive bids to ensure that it received the best value possible. While other features of the ceremony were also within the latitude allowed by the applicable regulations, the overall costs were unnecessarily costly.

In addition, at the end of FY 2003, TSA distributed $1,450,000 in individual cash awards to 88 TSA executives in conjunction with their FY 2003 performance evaluations. Seventy-six percent of its eligible executives received performance based cash awards, which put TSA in the top quartile of all federal agencies. The average amount paid to TSA's executives was 25% more than the average performance based cash awards given to federal executives government-wide. Moreover, the OIG found that identical, boilerplate language was used to justify awards to 38% of the awardees. Finally, TSA provided data that suggests that a significant disparity exists between its cash awards to its executives and its lower salaried employees. (OIG-04-046, September 2004, ISP)

A Review of the Use of Alternative Screening Procedures at an Unnamed Airport

The OIG reviewed allegations that an airport may have been using an unauthorized procedure to screen checked baggage. The OIG's review assessed whether the airport screened checked baggage according to applicable laws and TSA standards, and whether any alternative procedures used maintain security effectiveness and efficiency.

The reviewed airport used a TSA approved alternative screening procedure, a variation of explosive trace detection. At times, TSA does not screen checked baggage according to its standard operating procedures because it has insufficient equipment and human resources to adjust to high passenger volume, equipment unavailability, or other issues. For these situations, TSA approved several alternative screening procedures which the Aviation and Transportation Security Act authorizes. The reviewed airport used an alternative procedure primarily because it did not have sufficient space or equipment to adapt to passenger volume at peak times. Airport layout improvements and the installation of additional equipment in 2003 decreased the airport's use of the procedure.

Although the alternative procedure is authorized, the OIG has concerns about its use. TSA provided inadequate guidance to standardize screeners' use of the procedure, and the OIG encountered variations in use that could diminish its effectiveness. In addition, TSA headquarters lacked accurate records of the reviewed airport's use of alternative screening procedures throughout 2003. The OIG recommended that TSA revise the policy and program for alternative screening procedures, including improved reporting requirements. (OIG-04-028, July 2004, ISP)

Evaluation of TSA's Contract for Installation and Maintenance of Explosive Detection Equipment at United States Airports

As part of its review of the federalization of airport security screeners and the management of major DHS procurements, the OIG reviewed DHS' contract with the Boeing Service Company. Issues arose as to whether the contract was properly administered as a cost-plus-award-fee-contract and whether the level of profits paid to Boeing was reasonable. The OIG found that:

- Until December 2003, TSA paid contract fees based on a percentage of total invoiced costs, which had the effect of creating a cost-plus-a-percentage-of-cost type contract. This type of contract is prohibited in the federal government.

- The contract did not contain an award fee determination plan to evaluate the contractor's performance until December 2003, eighteen months after contract award, and it included cost increases unrelated to approved scope changes in the calculation of the award fee pool. Through December 2003, TSA had paid more than $44 million in provisional award fees without any evaluation of the contractor's performance.

- The profit paid to the contractor was disproportionately high when compared to the contractor's cost and risk and compared to what other agencies allow as

profit under such contracts. Based on these factors, OIG concluded that TSA paid Boeing at least $49 million in excess profit.

As a result of these findings, the OIG recommended that TSA's Director, Office of Acquisition:

- Reform the contract to avoid even the appearance that it is a cost-plus-a-percentage-of-cost type contract;
- Amend the award fee plan in the contract to ensure that the award fee pool does not include cost increases unrelated to approved scope changes;
- Evaluate Boeing's past performance based on the award fee plan and, if warranted, adjust the award fee accordingly;
- Recoup any unreasonable fees paid under the contract; and
- Develop guidance for the determination of reasonable base and award fees on cost-plus-award-fee-contracts.

While TSA recognized the shortfalls that exist in the administration of this contract, they took exception to the OIG's finding that the profit paid to the contractor was unreasonable. TSA does not plan to recoup any fees already awarded other than those fees associated with unwarranted cost growth. (OIG-04-044, September 2004, OA)

Review of the TSA Passenger and Baggage Screening Pilot Program

The Aviation and Transportation Security Act of 2001 (Public Law 107-71) required TSA to assume control of security screening at the nation's airports and to implement a two-year private security screening pilot program designed to determine whether, with proper government supervision and controls, contract screening companies could attain or exceed the performance levels provided by TSA's federal screener workforce. On October 10, 2002, TSA awarded four pilot program contracts covering five different airports. The pilot program began at the airports on November 19, 2002.

The OIG identified two primary weaknesses with TSA's passenger and baggage screening pilot program: the hiring, staffing, and training of screeners remained either completely or partially under the control of TSA, which limited the opportunities for the pilot contractors to test new innovations and approaches in these areas; and TSA did not have

criteria for evaluating the performance of either the pilot program contractors or the federal screening workforce.

The OIG recommended that TSA: 1) establish a passenger and baggage screening pilot program that allows greater flexibility for both contractor and federally staffed airports to test innovations and new approaches in hiring, training, and managing screeners; and 2) develop measurable criteria to properly evaluate and compare the performance of both contractor and federal screening operations. (OIG-04-047, September 2004, OA)

Review of TSA Screening Practices in Houston, Texas

At the request of the Ranking Member of the House Select Committee on Homeland Security, the OIG conducted an inquiry into allegations related to the TSA passenger screening security program at the George Bush International and William P. Hobby Airports in Houston, Texas. The request was prompted by a TV news report citing statements by screeners at both airports that, among other things, TSA management encouraged screeners to ignore alarms signaling potentially dangerous items in checked bags. The OIG recommended that TSA provide guidance and training on what TSA managers, supervisors, and screeners are to do in certain circumstances. The findings and recommendation were presented to the committee in a sensitive security information report. (OIG-04-048, September 2004, OA)

Audit of Passenger and Baggage Screening Procedures At Domestic Airports

In response to concerns about the vulnerability of airplane passenger and baggage screening processes to terrorist activity, the OIG reviewed the aviation security screening function at selected domestic airports nationwide. The review consisted of hundreds of undercover tests of screening checkpoints and checked baggage at different categories of airports nationwide, to evaluate screener and equipment performance regarding the inspection of passengers and property for explosives and weapons. The OIG found that improvements are needed in the screening process to ensure that dangerous prohibited items are not carried into the sterile areas of heavily used airports or do not enter the checked baggage system. Although each undercover test was a discrete and unique event that challenged an individual screener to make judgments or perform specific actions in response to the unfolding test scenario, there are four areas that the OIG concluded were the cause of most of the test failures: training; equipment and technology; policy and procedures; and management and supervision.

The OIG recommended that TSA develop and implement a program of recurrent professional training to enhance screener performance. The recommended program

would require a mandatory minimum amount of documented, continuous professional training for each screener, and include testing to determine mastery of the material. The OIG also recommended that TSA aggressively pursue the development and deployment of innovations and improvements to aviation security technologies, such as the dual- or multi-view x-ray machine, which has the potential to provide screeners with high-resolution 3-D images that can be rotated on the screening monitor for optimal viewing; and backscatter x- ray technology, which offers a more effective and unambiguous means of detecting hidden weapons than a pat-down inspection. The OIG also made recommendations regarding screening checkpoint standard operating procedures that could increase the effectiveness of the screening process. In addition, the OIG recommended that TSA take appropriate steps to improve management and supervisory oversight of screeners, to ensure that screeners are meeting a high standard of performance, and that they are complying with established procedures at all times. TSA has begun to implement significant improvements since the conclusion of the OIG's testing. A classified report was issued to select Senate and House of Representatives Committees. (OIG-04-037, OA)

Five TSA Screeners Indicted for Theft

An OIG joint investigation with TSA and the Federal Bureau of Investigation (FBI) resulted in the arrest and indictment of five screeners for violating conspiracy and theft of interstate commerce laws. The investigation determined that the screeners would exchange and sell various stolen items and, in some instances, they were wearing the jewelry that they had taken from passenger luggage. During a search of one of their vehicles, several pieces of jewelry were recovered. During a search of another screener's residence, numerous items were recovered, including jewelry, electronic devices such as MP-3 players, DVD players, laptop computers, and digital cameras. One of the screeners agreed to cooperate and wore a body wire to record conversations with the other screeners. Prosecution is pending. (OI)

TSA Oversight Review

The OIG conducted an oversight review of the TSA, Office of Internal Affairs and Program Review (OIAPR). OIAPR is responsible for conducting internal investigations of TSA employee misconduct. The OIG conducted this review to determine whether OIAPR was investigating allegations of employee misconduct in a thorough and timely manner. The OIG reviewed a representative sample of each category of investigation closed between March 1, 2003, and February 29, 2004. The categories of investigations reviewed included: assault; abuse of authority; harassment and violence; computer crimes and misuse; conflicts of interest; extortion and corruption; drug, alcohol and prohibited items, firearms, fraud and false documentation; security and intelligence, theft; and

other general misconduct. The OIG concluded that TSA OIAPR internal investigations were thoroughly and vigorously pursued and reported to appropriate officials in a timely manner. (OI)

TSA Security Screening Supervisor Terminated for Theft

The OIG initiated an investigation into the allegation that a TSA security screening supervisor at an airport was submitting forged Overtime Authorization Requests (OARs) for overtime and compensatory time. The investigation determined that the TSA Security Screening Supervisor submitted fraudulent OARs totaling approximately $8,080.85 from October 17, 2003 through April 8, 2004. As a result of the investigation, the TSA security-screening supervisor has been terminated. On August 17, 2004, a three count indictment was filed, charging the former TSA security screening supervisor with theft/ embezzlement. Plea negotiations are ongoing. (OI)

TSA Training Coordinator Terminated for Disclosing Information

The OIG initiated an investigation into the allegation that a TSA training coordinator at an international airport was compromising the 100% Checked Baggage Screener Training Module Exam by providing copies of the final examination and answers to screeners prior to their exams. The TSA training coordinator admitted to the allegation. According to the TSA training coordinator, the screeners to whom he gave the exam (for their use as a future study guide) had already taken and passed the test. TSA was forced to cancel all future exams until a new exam could be developed. As a result of the investigation, the TSA training coordinator has been terminated from TSA. (OI)

TSA Security Screener Charged with Theft of Funds

The OIG initiated an investigation into an allegation that a TSA security screener at an airport stole $400 from a passenger's wallet during the initial screening process. The TSA security screener admitted his involvement in the theft of the funds and was charged with theft under $500. At the initial hearing, the TSA security screener pleaded not guilty. Judicial action continues. (OI)

TSA Security Screener Arrested for Theft

The OIG, the Drug Enforcement Administration (DEA), and a state police department initiated an investigation based on an allegation that a TSA security screening supervisor at the airport was stealing medications from passengers' luggage during the checked bags search. On July 13, 2004, marked narcotics were introduced into controlled luggage that

would be searched by the targeted TSA security screener. The TSA security screener ingested one pill from the marked narcotics and stole approximately 20 to 25 pills from an uninvolved airline passenger's baggage. The TSA security screener's actions were captured on a real time video surveillance camera. The TSA security screener was then arrested and charged with a single count violation of theft by a government employee. On July 20, 2004, the TSA security screener was indicted by the federal grand jury on a two-count indictment charging violations of theft and possession of narcotics without a prescription. The TSA security screener was arraigned on the indictments on July 27, 2004, and entered not guilty pleas to each count. Trial date is pending. (OI)

TSA Security Screener Arrested for Sexual Assault on a Child and Obscenity

The OIG initiated an investigation into an allegation that a TSA security screener assigned to an airport was under investigation by the local police department for child pornography. The TSA security screener was arrested on April 21, 2004, on state charges of sexual assault on a child and obscenity. The incidents that caused the current state charges to be filed against the TSA security screener are not associated with his work place, employer, or position. The preliminary hearing was waived and plea negotiations are ongoing. (OI)

TSA Supervisory Screener Falsified Background Information to Obtain Position

An OIG investigation determined that a supervisory screener at an airport failed to reveal that he had recently been the subject of an internal affairs investigation by his former employer. The TSA supervisor failed to disclose this information when the information was requested on the Office of Personnel Management's Standard Form 85-P. The TSA supervisor also provided false employer references in an effort to hide his negative employment history. On June 1, 2004, the TSA supervisor resigned in lieu of termination. The U.S. Attorney's Office declined prosecution in lieu of termination. (OI)

TSA Employee Charged with Theft

An OIG investigation determined that a TSA screener stole an airline passenger's cellular telephone from the passenger's checked luggage. The screener's illegal use of the telephone incurred charges of $2,483.67. A county district attorney's office charged the employee with theft of telecommunication service. The TSA employee was terminated on July 19, 2004, for stealing and using the passenger's cellular telephone. On July 21, 2004, the former TSA employee was sentenced to five years probation. (OI)

TSA Screener Found Guilty of Theft by a Public Servant

An OIG investigation determined that a TSA screener stole cash totaling over $500 from a passenger's luggage during the security screening process at an airport. A county district attorney's office prosecuted the case. On April 30, 2004, the TSA screener was found guilty of theft by a public servant, and was sentenced to eighteen months probation. (OI)

TSA Screener Terminated for U.S. Copyright Violations

An OIG investigation determined that a TSA baggage screener was producing and selling counterfeit DVD movies to TSA employees and airport workers at an international airport while on duty. The subject admitted that he knew it was against U.S. copyright law to copy and sell the DVDs, but he did it to make extra money. Federal prosecution was declined and the subject was subsequently terminated. (OI)

U.S. Immigration and Customs Enforcement (ICE)

Evaluation of the Federal Air Marshal Service

Federal Air Marshal Service (FAMS), originally part of the TSA, achieved the goals set by Congress to hire and train the required number of air marshals. FAMS has taken significant steps to establish organizational policies and procedures to fulfill its mission and support its increased workforce. FAMS is a well trained and professional workforce, though there were several deficiencies in the program.

These deficiencies involve FAMS policies governing background investigation and adjudication requirements, field office training, reservist selection, medical qualifications, disciplinary actions, and travel procedures. The level of the OIG's concern was heightened with the transfer of FAMS within DHS to ICE. FAMS joined ICE on

November 2, 2003, allowing a large number of ICE special agents to augment the current force of FAMS. This augmentation requires the Assistant Secretary of ICE to make several decisions regarding how ICE agents will be selected, trained, and deployed to support the safety of the flying public.

This report also examined issues involving flight coverage and assignment, which are discussed in a classified appendix not made publicly available. (OIG-04-032, August 2004, ISP)

ICE Civil Rights Violation

Detention and Removal Operations, ICE, reported the sexual abuse of a detainee perpetrated by an ICE contract employee correctional officer. The detainee was coerced into performing oral sex on the officer. The officer admitted to his supervisor his activity with the detainee and voluntarily terminated his employment as a result of his behavior and after submitting to a polygraph examination and being confronted with information that he had done this with a second detainee. In July 2004, the officer signed a plea agreement admitting to one count of sexual abuse of a ward. In August 2004, the officer pleaded guilty to the one count. Sentencing of the officer is pending. (OI)

FAM Official Arrested for Kidnapping

The OIG initiated an investigation into the allegation that a FAM, while off-duty, was arrested for kidnapping. The victim (a juvenile) claimed the FAM identified himself as a law enforcement officer and ordered him into his vehicle. The FAM then drove the victim to the victim's residence where the FAM confronted the victim's family. The FAM claimed that the victim was harassing his wife while he (the FAM) was at work or traveling. The FAM denied that he used his credentials to get the victim into his vehicle. The FAM signed a one-year pre-trial diversion agreement with the local district attorney's office in lieu of formal prosecution. The DOJ Civil Rights Division declined this investigation for prosecution. (OI)

ICE Special Agent Indicted for Taking Bribes

The OIG received an allegation that an ICE Special Agent accepted bribes to assist a naturalized citizen with the deportation of a business competitor and assisted his wife with her alien status. It was alleged that the ICE agent received $10,000 to deport the business competitor. It was further alleged that the agent received money to assist the naturalized citizen's wife with possible deportation proceedings as a result of criminal charges against her. The agent was indicted on four counts--two counts of bribery, one

count of receiving compensation, and one count of making a false statement. The agent was arrested and a trial is pending. (OI)

ICE Special Agent Arrested for Taking Bribes

An ICE Special Agent was arrested for accepting cash payments ranging from $5,000 to $10,000 in exchange for providing illegal aliens with Employment Authorization Documents. The agent was previously employed as an office automation clerk for the U.S. Citizenship and Immigration Services. He was arrested along with two "recruiters" and indicted. The agent pleaded guilty to conspiracy, six counts of immigration fraud, bribery, and nine counts of money laundering. It was determined that the ring received at least $605,000 from the sale of these fraudulent documents. He was sentenced to 52 months incarceration and agreed to the forfeiture of $59,000, five vehicles, and a plasma television. One of the recruiters pleaded guilty to conspiracy, five counts of immigration fraud, and illegal re-entry into the United States after previously being deported. He was sentenced to 30 months incarceration and agreed to the forfeiture of $5,900, a sailboat, jet skis, and six vehicles. The second recruiter was convicted and is scheduled to be sentenced this fall. (OI)

Federal Protective Service Police Officer Involved in a Fatal Shooting

The OIG received information that in November 2003, an Federal Protective Service police officer was involved in a fatal shooting incident. The incident was investigated by the local police department, with assistance by the OIG. The investigation determined that the victim, a 15-year-old juvenile, attacked and struck the off-duty officer in full uniform, with a crowbar and fists, causing injuries to his head and face. The officer, fearing for his life, drew his service weapon and fired two shots, which struck and killed the juvenile. The investigation found no evidence to indicate any wrongdoing by the officer. The matter was presented to the DOJ Civil Rights Division, which issued a Notice to Close File, stating that the case lacked prosecutive merit. The case was also declined by the local prosecutor's office with the finding that the officer had acted in self-defense. (OI)

ICE Special Agent Sentenced for Making False Statement in Application and Use of Passport

On August 26, 2004, an ICE special agent was sentenced to two years probation and ordered to pay a $100 special assessment fee and a $200 fine. The joint OIG/FBI investigation determined that the agent made a false statement in an application for a

passport with the intention of securing it for the use of someone else. The subject had worked as a federal law enforcement officer for over fifteen years. (OI)

ICE Officials Did Not Cause Detention Facility Death

An illegal resident alien from Mexico was arrested by a state police department on the basis of outstanding traffic warrants. At the time of his questioning by ICE, the illegal resident was behaving erratically and carrying no documentation, and he told ICE officials that he had entered the United States illegally. He was detained by ICE on June 24, 2004, and housed overnight at a county detention facility while ICE undertook an investigation to determine his status. Through the persistence of its investigative efforts, ICE developed information that he was likely a legal resident alien, and arranged for his release from detention on June 25, 2004. The alien became ill while detained at the county detention facility and, on the morning of June 25, 2004, before he could be released from custody, he was transported by ambulance to the medical center, where he died on June 28, 2004. The OIG reviewed the coroner's autopsy report, which concluded that the death was the result of natural causes. A review of the state police investigation found no evidence of prisoner abuse. The OIG investigation did not find any evidence of abuse by ICE employees. In fact, the investigation determined that the actions taken by ICE personnel were timely, prudent, and necessary to determine the alien's status. No evidence was found to indicate that the action of any ICE employee contributed to his death. (OI)

Customs and Border Protection

A Review of the Secure Electronic Network for Travelers Rapid Inspection Program

The Secure Electronic Network for Travelers Rapid Inspection (SENTRI) program permits pre-screened and enrolled low risk travelers to enter the United States from Mexico in designated lanes with minimal inspection by CBP officers, avoiding the lengthy waiting times in the regular inspection lanes. The SENTRI program is open to both United States citizens and certain non-citizens. The OIG determined that the program is generally achieving the two basic objectives for which it was established--accelerating the passage of participating travelers through land ports of entry, and maintaining border integrity, security, and law enforcement responsibilities.

However, the OIG noted several deficiencies that could compromise border security. Specifically, different land ports of entry applied eligibility criteria for criminal offenses, financial solvency, and residency differently. Also, there were apparent inconsistencies with application approvals and denials. In addition, the OIG noted weaknesses in the

procedures by which SENTRI system records are kept current, and how alerts are disseminated to CBP officers. CBP needs to develop criteria for random compliance inspections and improve its documentation for the results of compliance inspections, violations of SENTRI rules, and the administration of penalties. There is an absence of assessment and performance measures to support choices CBP has made involving the addition of SENTRI lanes at various land ports of entry. Taken as a whole, the OIG's findings indicate weak program management that could jeopardize the program's integrity and border security. (OIG-04-014, June 2004, ISP)

Review of Deemed Exports

The report addresses the DHS' involvement in the deemed export process. Deemed exports are the transfer of technical data to a foreign national that is considered to be an export of this data to the home country of the foreign national. The technical data is subject to the Export Administration Regulations and the International Traffic in Arms Regulations for dual use commodities and munitions, respectively. The deemed export information may take a tangible form such as a model, prototype or blueprint, or intangible form such as information learned by the foreign national.

This report is part of the fiscal year (FY) 2004 Interagency Review of Controls Over Deemed Exports, required by the National Defense Authorization Act for FY 2000 (Public Law 106-65), to assess the processes and procedures implemented to prevent the transfer of militarily sensitive technology to countries and entities of concern. The purpose of the OIG's review was to: 1) determine the roles and responsibilities of the various components of DHS involved in the deemed export process; 2) determine whether DHS policies and procedures foster compliance with deemed export requirements; 3) determine whether these procedures provide a reasonable level of assurance that controlled technologies or technical information are adequately protected and not released to foreign nationals inappropriately; and 4) follow up on prior year recommendations.

Current policies and procedures do not explicitly foster compliance with deemed export requirements, and thus do not provide a reasonable level of assurance that controlled technologies or technical data are adequately protected and not released to foreign nationals inappropriately. The OIG made recommendations to address weaknesses in the deemed export process. (OIG-04-023, April 2004, OA)

Effectiveness of Customs and Border Protection's Procedures to Detect Uranium in Two Smuggling Incidents

At the request of Congressman John Dingell, the Ranking Member, House Committee on Energy and Commerce, and, Congressman Jim Turner, Ranking Member, House Select Committee on Homeland Security, OIG conducted a review of CBP's efforts to detect depleted uranium in two smuggling incidents initiated by ABC News. In both incidents, reporters were successful in smuggling depleted uranium in to the U.S. via commercial shipping containers.

OIG found several weaknesses that occurred at the time of the two incidents that made the container inspection process less effective. The protocols and procedures that CBP officials followed at the time of the two smuggling incidents were not adequate to detect the depleted uranium. CBP has since enhanced its ability to screen targeted containers for radioactive emissions based on deployment of more sensitive technology, better procedures, and training, in response to OIG recommendations. (OIG-04-040, September 2004, OA)

Mobile Vehicle and Cargo Inspection System examining oceangoing cargo containers at Long Beach (shows cranes and containers stacked on ship in background)

Inspector using a Radiation Isotope Identification Device on an oceangoing container that is loaded onto a truck chassis.

A closer view of the Radiation Portal Monitors (RPMs) operating at the Global Marine Terminal at Newark

Audit of the Automated Commercial Environment Secure Data Portal: Security Requirements Need To Be Implemented

The development of the Automated Commercial Environment (ACE) is a massive and multifaceted effort directly related to the success of the CBP mission. The goal of ACE is to create a single portal for all federal requirements for international cargo. This will benefit the trade community by providing a single web-based interface to make periodic payments, post transactions, and view statement records by account. The federal government will benefit from the creation of a common knowledge-based risk management system for joint enforcement targeting and intelligence development.

The OIG's audit was conducted to ensure that basic security controls were in place before the system is moved into production and becomes available to users. The OIG tested the basic security features and found system weaknesses that needed to be corrected. These basic security requirements need to be in place to have proper safeguards and reduce exposure to risks from individuals or groups with malicious intent. The goal of ACE is to

allow the federal government to provide a "single window" on border cargo regulation to reduce the complexity, redundancy, and burden on the trade. The CBP plans for ACE to be a customer-oriented, account-centric process that provides real-time access to internal and external revenue, sensitive law enforcement, and proprietary corporate information through a secure global channel for travel and trade. CBP agreed to have all basic system security requirements in place prior to continuing the project. (OIG-04-022, May 2004, OA)

Audit of the Automated Commercial Environment Secure Data Portal: Management Controls Needed Improvement

The objective of the audit was to determine whether the ACE Secure Data Portal was being managed and developed to meet user expectations in the areas of user feedback and the change request process. The process used by e-Customs Partnership (eCP) to gather user feedback was adequate. During a 90-day pilot, eCP established a logical process to gather user feedback. This process resulted in the initiation of Product Trouble Reports (Trouble Reports), and change requests. However, the CBP Modernization Office was not tracking all the user feedback collected by eCP. A monitoring process would allow the CBP Modernization Office to review, evaluate, monitor, and track user feedback to ensure that issues important to CBP are properly addressed. In addition, change request packages did not always have the required documentation identifying how changes would affect the program. As a result, the Change Control Board and Project Directors approved work requirement changes without knowing the full impact of the changes to the program. (OIG-04-035, September 2004, OA)

CBP Canine Enforcement Officer Arrested for Narcotics and Child Pornography

The OIG conducted a joint investigation with ICE OPR and the FBI Corruption Task Force into the allegation that a CBP canine enforcement officer was passing narcotics laden vehicles through the Nogales, Arizona port of entry. The investigation resulted in the arrest of the canine officer after he took possession of two kilograms of cocaine. A search of his home led to the discovery and seizure of numerous weapons, chemicals used to manufacturer explosives, and in excess of 30,000 images of child pornography. Videos were discovered that revealed that the canine officer had been sexually active with his daughter since she was the age of three. The local sheriff's department has joined the investigation and is reviewing the evidence for criminal violations of state sexual conduct laws. The canine officer was indicted by a federal grand jury for violations of federal narcotics and child pornography laws. The canine officer's wife was also indicted for violations of federal narcotics laws. (OI)

Contract Border Patrol Agent (BPA) Employee Arrested on a State Charge of Aggravated Sexual Assault

The OIG received information that suggested that a contract BPA employee was having sexual relations with the 15-year-old daughter of a DHS employee. The information also suggested that the employee had induced the girl to make sexually explicit images of herself, and to email those images to the employee's web based email account. It was further suggested that the employee downloaded these images on computers located at his residence and on government owned computers at work. During an interview with OIG, the employee confessed to the allegations. He admitted to knowing the girl was underage, and to having sexual relations with her. The employee further admitted to inducing the girl to take sexually explicit images of herself, and emailing those images to him, the majority of which he admitted to viewing at work. Following his admission, the employee was arrested on a state charge of aggravated sexual assault. (OI)

CBP BPA Arrested for Violating a Condition of His Release

An OIG investigation was initiated based on information from the Texas Department of Public Safety that a former BPA displayed a BPA badge during a traffic stop. The BPA had been previously convicted of Deprivation of Rights Under Color of Law and was sentenced to 27 months imprisonment. The BPA appealed his conviction and was released on an unsecured bond. The OIG determined that the BPA stole the badge from the CBP, and later displayed the badge during a traffic stop. The BPA was arrested for having violated a condition of his release and was then sentenced to the original 27-month sentence. (OI)

Private Attorney Arrested for Impersonating A Federal Officer

The OIG and the Internal Revenue Service's (IRS) Criminal Investigation Division conducted a two-year joint investigation of a private attorney, who attempted to board an airplane with a concealed, loaded handgun after claiming to be a U. S. Customs Service employee. In 2003, the attorney falsely presented himself as a DHS employee in an attempt to purchase an airline ticket at a federal government discounted rate. On June 25, 2004, the attorney was arrested for impersonating a federal officer and attempting to board a commercial aircraft with a firearm, in addition to making a false statement on a loan application, witness tampering, and tax evasion related to his law practice. As a result of this investigation, the attorney has relinquished his law license. Trial has been scheduled for December 2004. (OI)

CBP Senior Border Patrol Agent Charged with Official Oppression

An OIG investigation was initiated based on information that a senior Border Patrol agent harassed a woman after a traffic stop. The OIG investigation determined that the agent violated established INS and CBP policies and procedures. The agent did not advise anyone that he was transporting a single woman for a period of two hours, during which time he inappropriately touched her. The agent then released the woman after determining that she was in violation of immigration law. The local district attorney's office issued an arrest warrant charging the agent with Official Oppression. Judicial action is pending. (OI)

CBP Officer Indicted for Civil Rights Violation

An OIG joint investigation with ICE OPR resulted in a CBP officer's being indicted for violation of Deprivation of Rights Under Color of Law. This was as a result of an assault by the officer of a Chinese tourist. Judicial action continues. (OI)

CBP Inspector Arrested for Stealing State Government Property

An OIG joint investigation with a police department resulted in the arrest of an immigration inspector at an international airport. The OIG initiated an investigation into an allegation that a CBP immigration inspector traveled on a commercial aircraft, while off-duty, carrying a firearm. During this investigation, the subject was observed operating a vehicle that had the appearance of a law enforcement vehicle. The vehicle was also found to have an undercover law enforcement license plate attached. The investigation determined that this vehicle was the subject's privately owned vehicle, and the undercover license plate should not have been in his possession. During an unrelated surveillance, the subject was observed breaking into a marked police vehicle and stealing an airport "All Access" pass. The subject was arrested and charged in connection with theft. Trial is pending. (OI)

Theft of Funds from CBP Safe

In April and August 2003, CBP employees reported to OIG that funds in the amount of $10,000 and $15,000, respectively, were discovered missing from the CBP safe at an international airport. The funds were inventoried on multi-copy property receipts, placed into security pouches with a copy of the receipts, secured with numbered security seals, and placed in the CBP safe. The investigation determined that CBP has a policy for processing valuables held and inventoried while aliens or other people are detained. The policy requires the maintenance of a log to record the placement of items in the safe. The

logs are not standardized, maintained consistently, accurately or securely, and parts of the logs were discovered missing. Local policy required an audit of the log and contents of the safe at the beginning of each shift. However, the audits were not performed, so the thefts went undetected for an undetermined period of time. Further, the safe was left open for undetermined periods of time, allowing all CBP employees access. The OIG report recommended ten corrective actions to prevent further thefts and/or losses from the CBP safe. (OI)

Export Brokers Attempt to Bribe CBP Inspectors

A cooperating CBP inspector told OIG that he had been approached by a local export broker and offered a bribe to expedite the documentation of several vehicles awaiting export to Mexico. The OIG conducted a seven month undercover operation and recorded (audio/video) meetings with several export brokers who said that the inspector had expedited the export documentation of vehicles for a fee. A pro-active operation was conducted with the assistance of the cooperating inspector. A total of 18 export brokers and one National Insurance Crime Bureau (NICB) employee were recorded (audio/video) bribing the cooperating inspector. On February 26, 2004, a total of 18 export brokers representing seven brokerage houses and one NICB employee were indicted by a federal grand jury for 53 counts of bribery. On August 3, 2004, the NICB employee pleaded guilty to three counts of bribery. Sentencing is scheduled for October 18, 2004. The first trial of four brokers is scheduled to begin later this year. (OI)

Five CBP Immigration Officers Arrested for Alien Smuggling

After an extensive OIG investigation, five immigration detention officers were arrested, pleaded guilty, and convicted of conspiring to bring a woman into the United States without the proper documentation. The officers shielded the woman from detection. CBP officers encouraged the woman to cross the border into Texas. One of the federal immigration officers transported her from one location to another with the help of other officers. Two of the officers knew about the illegal activity but failed to report it. On April 23, 2004, four of the subjects were sentenced to 24 months probation and 200 hours of community service each. On August 3, 2004, the fifth subject received the same sentence. (OI)

CBP Customs Inspector Arrested on Bribery Charges

An inspector with the U.S. Customs and Border Protection was arrested and indicted on drug and bribery charges. The federal grand jury charged the inspector with conspiracy to import over 5 kilograms of cocaine and bribery. On June 11, 2004, the inspector allowed

cars loaded with cocaine to enter the U.S. from Mexico without inspection in exchange for $6,000. The OIG, the FBI, and CBP are conducting a joint investigation. If convicted, the inspector faces between 10 years to life in a federal prison on the drug conspiracy charge and up to 15 years on the bribery charge. (OI)

CBP Employee Exonerated

On July 13, 2004, the FBI provided the OIG with a Suspicious Activity Report filed on a BPA by a bank. The report documented that a BPA walked into the bank on May 20, 2004, and attempted to deposit $20,000 cash, wrapped in duct tape, into his personal savings and checking account. When initially questioned by the bank, the BPA quickly departed the bank. The OIG investigation determined that the $20,000 was proceeds from a construction loan for which the BPA had applied and subsequently received and was not the result of criminal activity. (OI)

CBP Detention Officer Exonerated of Civil Rights Violation

An OIG investigation was initiated based on a complaint that a Nigerian national awaiting deportation was severely beaten by a Detention Officer at a detention facility. The OIG investigation determined that there was no evidence to support the allegation against the officer. The U. S. Attorney's Office declined prosecution. The Nigerian national is scheduled for deportation to Nigeria in late September 2004. (OI)

Senior BPA Exonerated of Civil Rights Abuse

On June 22, 2004, the OIG received information that a Mexican national alleged that he had sustained injuries to his left ankle when a senior BPA purposely ran over his leg with the agent's service vehicle. The complainant subsequently recanted his accusation in a sworn statement. The attending physician opined that the complainant's injuries appeared to be caused by a fall, rather than by an automobile crushing his foot. A breathalyzer test conducted by the police department, revealed that the complainant had a blood alcohol content of .22% at the time of his arrest, which is nearly triple the legal limit in the state. Both the United States Attorney's Office and the Civil Rights Division, Criminal Section, United States Department of Justice, Washington, D.C., declined prosecution for a violation of Deprivation of Rights Under Color of Law. The OIG investigation into this matter determined that the agent took no improper action and that the claim made by the complainant was unfounded. (OI)

BPA Exonerated of Deprivation of Rights Under Color of Law

The OIG received an allegation that a BPA used excessive force while apprehending the driver of a car full of illegal aliens. The complainant had no visible injuries and never requested medical treatment. The complainant did not make his allegation until several hours after his arrest, when he was being processed for admittance to the processing center. While being processed at the border patrol station, the complainant told several lies to the processing agents, including ones about his previous arrest record, his identity, and his role as driver of the car. While being interviewed by OIG agents, the complainant said that a pre-existing injury had been aggravated by the arrest, but that the agent did not use excessive force. The complainant refused to give a sworn statement, and said that he wished to withdraw his allegation. Two other BPAs were present during the arrest. Neither of them witnessed any abuse. The video footage obtained by Border Patrol Remote Video Surveillance Cameras did not depict any use of force by any agent. The OIG found no substantiation for the allegation of abuse. (OI)

CBP BPA Exonerated of Abuse

The OIG received information from an illegal alien who alleged that he was abused when apprehended by CBP in September 2003. The alien's attorney alleged that his client had been kicked and beaten, resulting in broken ribs and his eye swollen shut. A review of apprehension records indicated that the illegal alien, when apprehended, had a swollen, infected eye, and that he was treating the infection with eye drops. The illegal alien was provided with medical treatment. A review of the medical treatment disclosed that chest x-rays showed no broken ribs and that the alien in fact had a bad infection of his eye resulting in the eye's being swollen shut. Additionally, the records showed that the illegal alien had no broken facial bones. (OI)

CBP Senior Official Cleared of Favoritism Allegations

An OIG investigation was initiated after an anonymous complainant alleged favoritism on the part of a CBP senior official. The alleged favoritism involved hiring practices, promotions, and the granting of "special privileges." The subsequent OIG investigation, which involved numerous witness interviews and the interview of the senior official, determined that the allegations were unfounded. (OI)

United States Citizenship and Immigration Services

CIS District Adjudications Officer Arrested for Charging and Collecting Unauthorized Fees in Naturalization Proceedings

The OIG and the FBI initiated an investigation into the allegation that a District Adjudications Officer in an office of the CIS was extorting money from immigration applicants. In April 2003, the officer told a Chinese national attempting to obtain U.S. citizenship that he would have no problem if he paid the officer $2,000. The victim paid $1,000, and was told to pay the remainder of the money in May 2003. On May 6, 2003, the OIG and the FBI observed the officer accepting a $1,000 bribe from the victim. The officer was arrested on February 26, 2004, by OIG and the FBI, and was subsequently charged with two counts of Charging and Collecting Unauthorized Fees in Naturalization Proceedings. Plea negotiations are ongoing. (OI)

CIS Employee Pleads Guilty to Mail Fraud in Embezzlement Scheme

An OIG investigation determined that a CIS Examinations Assistant embezzled funds from a federal employee's organization of which the employee served as an officer. The CIS employee had access to the employee organization's bank account, and over a five-month period withdrew over $32,000 in cash and money orders for personal use. The investigation was accepted for prosecution by the United States Attorney's office and on February 25, 2004, the employee was indicted on five counts of mail fraud. On April 8, 2004, the immigration employee pleaded guilty to one count of mail fraud, and was sentenced to eight months incarceration. The CIS employee was terminated prior to sentencing. (OI)

CIS Employee Charged with Disclosure of Sensitive and Confidential Information

An OIG investigation determined through electronic surveillance that a CIS contract employee provided case related information to the subject of an Organized Crime Drug Enforcement Task Force investigation. The employee confessed and provided a sworn written statement. The employee was immediately terminated. The U.S. Attorney's Office filed an indictment against the contract employee for disclosure of sensitive and confidential information. Judicial action is pending. (OI)

An Immigration Information Officer Arrested for Taking Bribes

An OIG joint investigation with ICE received information from a confidential informant that an Immigration Information Officer was accepting cash payments in exchange for

providing illegal aliens with travel permits, paroles, and ADIT stamps (used on foreign passports). In an undercover operation, the officer accepted $8,000 and seven passports and subsequently placed ADIT stamps in the passports. The officer was arrested and pleaded guilty to bribery and immigration fraud and is scheduled to be sentenced in October 2004. (OI)

Former INS Employee Arrested for Bribery, and Alien and Drug Smuggling

On May 17, 2004, a former INS inspector was arrested by the OIG. The subject, along with nine civilians, was previously indicted on charges of bribery, and alien and narcotics smuggling. The investigation was worked jointly with the local Border Corruption Task Force, consisting of members from the FBI, DEA, IRS, ICE and OIG. The investigation identified a smuggling organization based in Mexico. This organization's inner circle was identified as family members who lived in Mexico and the U.S. Through the use of informants, surveillances and undercover operations, the investigation disclosed that the INS Inspector was being paid $5,000 - $10,000 per vehicle by the organization to allow illegal aliens and narcotics into the U.S. without proper inspection. On May 24, 2004, several of the organization's family members were arrested. On August 10, 2004, another family member surrendered to OIG and the FBI. Another member is currently in Mexico and is not expected to surrender to U.S. authorities. Most of the individuals are cooperating and are providing information on other smuggling organizations and corrupt activities. (OI)

CIS Information Officer Indicted for Bribery

An OIG joint investigation was conducted with the DOJ OIG and the FBI into allegations that an information officer with the CIS had accepted bribes to allow illegal aliens to enter the United States. The OIG investigation concluded that from 1998 through 2001, in exchange for bribes, the officer used various methods to circumvent INS procedures and allow the entry of illegal aliens, including the advance parole of aliens (Form I-512), fictitious creation of alien files, and unauthorized approval of Application to Replace Permanent Residence Card (Form I-90). His actions resulted in the illegal entry of more than 100 people. He was indicted and subsequently pleaded guilty to one count of conspiracy to smuggle illegal aliens into the United States and one count of bribery. In April 2004, he was sentenced to 22 months in custody of the Attorney General. The OIG investigation into the actions of his civilian co-conspirators is ongoing. (OI)

Information Analysis And Infrastructure Protection (IAIP)

Progress and Challenges in Securing the Nation's Cyberspace

DHS has begun to implement the actions and recommendations detailed in *The National Strategy to Secure Cyberspace (NCSD)*. With the establishment of NCSD in June 2003, DHS made notable progress in protecting the nation's critical infrastructure from cyber vulnerabilities, threats, and attacks. Major accomplishments include:

- creation of the United States Computer Emergency Readiness Team (US-CERT). Formed as a partnership between NCSD and the private sector, US-CERT serves as the national focal point for computer security efforts.
- establishment of the National Cyber Alert System, managed by US-CERT, as the means to relay cyber security information to all computer users.
- participation by NCSD in Dartmouth College's cyber focused communications and coordination exercise (LiveWire).
- sponsorship by NCSD of the National Cyber Security Summit to promote information sharing and partnerships with the private sector in securing cyberspace.
- formation of three new organizations to strengthen federal information technology defenses and coordinate responses to system threats.

Though NCSD has undertaken some major initiatives, it still faces a number of challenges to address long-term cyber threats and vulnerabilities to the nation's critical infrastructure. Specifically, NCSD has not:

- prioritized its initiatives to address the recommendations in *The National Strategy to Secure Cyberspace.*
- identified the resources needed to ensure that it can identify, analyze, and reduce long-term cyber threats and vulnerabilities.
- developed strategic implementation plans, including performance measures and milestones, focusing on the division's priorities, initiatives, and tasks.

- instituted a formal communications process within DHS, as well as the public, private, and international sectors.

- initiated and implemented a process to oversee and coordinate efforts to develop best practices and create cyber security policies with other government agencies and the private sector.

- reviewed or updated the actions and recommendations in *The National Strategy to Secure Cyberspace.*

NCSD must address these issues to reduce the risk that the critical infrastructure may fail due to cyber attacks. IAIP agreed with and has already taken steps to implement each of the recommendations. (OIG-04-029, July 2004, IT)

DHS Challenges In Consolidating Terrorist Watch List Information

DHS is not playing a lead role in consolidating terrorist watch list information. Instead, these consolidation activities are generally administered by the entities that were responsible for collecting and disseminating terrorist information prior to DHS' formation. DHS officials said that the new department lacked the resources and infrastructure to assume responsibility for the consolidation. While DHS asserted that Homeland Security Presidential Directive – 6 precludes the department from leading the consolidation effort, the OIG disagrees and believes that DHS has a legal obligation to play a more robust role than at present by overseeing and coordinating watch list consolidation activities across agency lines. Such oversight would help DHS fulfill the role required by the Homeland Security Act and better ensure that the past ad hoc approach to managing watch list consolidation is not continued.

Stronger DHS leadership and oversight would also help improve current watch list consolidation efforts. Although some progress toward streamlined processes and enhanced interagency information sharing has been made, the consolidation is hampered by a number of issues that have not been coordinated effectively among interagency participants. Specifically, in the absence of central leadership and oversight for the watch list consolidation, planning, budgeting, staffing, and requirements definition continue to be dealt with on an ad hoc basis, posing a risk to successful accomplishment of the goal. (OIG-04-031, August 2004, IT)

Emergency Preparedness and Response (EP&R)

The Federal Emergency Management Agency's Individual and Family Grant Program Management at the World Trade Center Disaster

Newspaper articles reported that the Individual and Family Grant (IFG) program after the World Trade Center Disaster was "rife with fraud and abuse," and that 90 percent of the applications for air quality items were filed by people not suffering from the effects of contaminated air. Representatives Carolyn B. Maloney and Jose Serrano requested an audit into the allegations.

The OIG concluded that FEMA and state officials took several actions related to air quality items that, while consistent with FEMA regulations, reduced managerial controls and increased the risk of abuse. Such actions included eliminating home inspections for air conditioners and authorizing advance payments to applicants who were financially unable to purchase air quality items. These decisions, exacerbated by misleading advertising campaigns by companies selling air quality items, greatly increased the number of apparently fraudulent applications.

Once the problems were identified, FEMA and the state took action to address suspected fraudulent applications. FEMA program officials selected two samples of applicants to conduct home inspections--one of applicants who applied for assistance to buy window air conditioners, and one to verify whether cash advances were applied for properly. While the claim that ninety percent of applicants for air quality items were filed by people not suffering from the effects of contaminated air was probably overstated, the number of questionable applications based on the sample was high, as much as 62 percent for those applying for air conditioners. FEMA OIG investigated a number of alleged instances of fraud and referred several for prosecution. While no abuse should be tolerated, OIG found no evidence that problems within the IFG program caused any eligible New York citizens not to receive needed air quality items.

The OIG recommended that FEMA, when faced with a similar situation in the future, require the state to select individual applicants randomly on a regular basis, and take whatever action is appropriate to verify their eligibility. FEMA concurred with this recommendation. (OIG-04-049, September 2004, OA)

Dekalb County, Georgia, Questioned Disaster Costs

The county received an award of $12 million from the Georgia Emergency Management Agency to provide emergency protective measures and remove debris as a result of

damages caused by a severe ice storm. The OIG questioned costs of $161,352 resulting from unsupported, excessive, and ineligible project charges contained in the county's claim. (DA-23-04, May 6, 2004, OA)

Massachusetts Bay Transit Authority

The Authority received an award of $31.8 million from the Massachusetts Emergency Management Agency to remove debris, pump water from the subway system, and repair the electrical and signal systems damaged as a result of a flood. The OIG questioned costs of $623,938 resulting from work not implemented and unauthorized, unrelated, unsupported, and duplicative charges contained in the agency's claim. (DA-28-04, June 10, 2004, OA)

University of the Virgin Islands

The University of the Virgin Islands received an award of $4.4 million from the V.I. Office of Management and Budget for debris removal, emergency protective measures, and repairing and providing code upgrades to buildings damaged as a result of Hurricane Marilyn. The OIG questioned costs of $1,818,638 resulting from charges for building repairs that were covered by insurance but included in the university's claim. (DA-30-04, June 30, 2004, OA)

North Carolina Division of Parks and Recreation

The division received an award of $10.4 million from the North Carolina Division of Emergency Management to remove debris, provide emergency protective measures, and to repair facilities damaged as a result of Hurricane Fran. The OIG questioned costs of $7.3 million resulting from unsupported costs, unauthorized work, pre-disaster damages, and mathematical errors included in the division's claim. (DA-33-04, August 13, 2004, OA)

Texas' Compliance With Disaster Assistance Program's Requirements

Foxx & Company, an independent accounting firm under contract with the Office of Inspector General, reviewed the disaster grants management system and practices of the State of Texas, Texas Division of Emergency Management (TDEM). The overall objective of this audit was to determine the effectiveness of TDEM's administration and management of disaster assistance programs authorized by the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Public Law 93-288, as amended) and applicable federal regulations. On October 30, 2000, the President signed the Disaster Mitigation

Act of 2000 (Public Law 106-390). This Act was not fully implemented by FEMA at the time of the audit.

The audit concluded that the State of Texas, for the most part, had effectively managed FEMA disaster assistance program funds in accordance with federal requirements. However, some weaknesses in internal controls and non-compliance situations were identified. The report includes recommendations that, if implemented properly, would improve TDEM's management, eliminate or reduce weaknesses in internal controls, and reduce instances of non-compliance with federal laws and regulations. (DD-11-04, July 30, 2004, OA)

Minnesota's Compliance With Disaster Assistance Program's Requirements

Cotton & Company LLP, an independent accounting firm under contract with the OIG, reviewed the disaster grants management system and practices of the State of Minnesota, Division of Homeland Security and Emergency Management (HSEM). Primary audit objectives were to determine whether HSEM administered FEMA disaster and emergency programs according to federal regulations, properly accounted for and used FEMA program funds, and submitted accurate financial expenditure reports.

The audit identified program management findings related to the Hazard Mitigation (HM), Public Assistance (PA), and the IFG programs, as well as financial management issues primarily related to PA and HM grant management costs. (DD-14-04, August 13, 2004, OA)

City of St. Peter, MN

The OIG audited $9.9 million in FEMA public assistance funds awarded to the City of St. Peter, Minnesota. The City received the award for damages caused by severe storms and tornadoes on March 29, 1998.

The City did not follow federal procurement regulations in contracting for $8,931,295 in debris removal work. As a result, fair and open competition did not occur and FEMA had no assurance that contract costs claimed were reasonable. Additionally, the City did not expend and account for FEMA funds in accordance with federal regulations and FEMA guidelines. Consequently, the OIG questioned $2,032,333 ($1,524,250 FEMA share) in claimed costs; consisting of unreasonable costs, duplicate benefits, and ineligible labor costs. (DD-15-04, August 17, 2004, OA)

Hempstead County, Arkansas

The OIG audited $10.79 million in FEMA public assistance funds awarded to Hempstead County, AR. The County received the award for damages caused by severe ice storms on December 12, 2000.

The County accounted for and expended $9,975,777 of contract costs claimed for debris removal according to federal regulations and FEMA guidelines. However, the County's records did not adequately support $539,412 ($404,559 FEMA share) of costs claimed for road repair projects completed by County employees. Further, the Arkansas Department of Emergency Management overpaid the County $610,530 in federal grant funds, on which the County earned $16,954 of ineligible interest. Accordingly, the OIG questioned a total of $1,166,896. (DD-12-04, August 6, 2004, OA)

Michigan State Police, Emergency Management Division, Lansing. Michigan

The OIG audited $19.86 million in public assistance funds awarded to the Michigan State Police, Emergency Management Division, Lansing, Michigan for damages caused by severe windstorms on May 31, 1998.

The Michigan State Police did not account for and expend FEMA funds according to federal regulations and FEMA guidelines. Michigan State Police's claim included $4,492,408 ($3,402,632 FEMA share) of costs that the OIG found questionable. The questioned costs included unreasonable contractor profits, ineligible mobilization costs, ineligible sub grantee administrative allowance, unsupported engineering costs, and ineligible travel costs. (DD-09-04, June 16, 2004, OA)

Minnkota Power Cooperative, Inc., Grand Forks, ND

The OIG audited $6.76 million in FEMA public assistance funds awarded to the Minnkota Power Cooperative by the North Dakota Division of Emergency Management. The Minnkota Power Cooperative received the award for snow and ice related damages that occurred in March through July, 1999.

The OIG questioned costs of $621,590 that were included in the City's claim. These questioned costs included unsupported contract equipment costs ($492,155), ineligible contract labor and equipment costs ($104,910), unsupported contract labor costs ($12,288), and unreasonable costs on "cost-plus" contracts ($12,237).

Further, Minnkota Power Cooperative did not follow federal procurement regulations in contracting for $4,006,934 in disaster work. As a result, fair and open competition did not occur, and FEMA had no assurance that contract costs claimed were reasonable. (OIG-DD-01-04, October 29, 2003, OA)

City of Kelso, Washington

The City received an award of $5.2 million from the State of Washington Military Department's Emergency Management Division for damage caused by excessive rains that resulted in landslide activity. The OIG identified $3,619,164 in questionable costs, consisting of $3,499,231 for an ineligible alternate project election, and $119,933 of other federal funds the City improperly applied to meet its cost-sharing requirement. (OIG-DS-19-04, August 6, 2004, OA)

Wyoming State Forestry Division, Cheyenne, WY

The OIG audited $2.67 million in FEMA fire suppression assistance funds awarded to the Wyoming State Forestry Division (SFD). SFD received the award for damages resulting from the Green Knoll forest fire in July 2001.

SFD did not expend and account for FEMA funds according to federal regulations and FEMA guidelines. The OIG questioned costs of $341,294 that were contained in SFD's claim. The questioned costs (100 percent FEMA share) consisted of unsupported costs based on estimates ($316,167), ineligible land rehabilitation costs ($14,617), and unsupported equipment costs ($10,510). (OIG-DD-05-04, December 11, 2003, OA)

Santa Clarita Health Care Association, Santa Clarita, CA

The Association received an award of $16 million from the California Office of Emergency Services for damages caused by the Northridge earthquake. The OIG identified $2,290,275 in questionable costs consisting of duplicate benefits, ineligible project costs, excessive project management costs, and unsupported project costs. (OIG-DS-12-04, May 7, 2004, OA)

King County, Seattle, WA

The County received an award of $4.6 million from the State of Washington, Emergency Management Division for damage caused by flooding. The OIG identified $527,918 in questionable costs consisting of ineligible ground stabilization costs, ineligible project

charges, excessive force account equipment charges, accounting errors, and unsupported costs. (OIG-DS-16-04, July 27, 2004, OA)

City of Seattle, WA

The City received an award of $5 million from the State of Washington, Emergency Management Division for damage caused by flooding. The OIG identified $409,264 in questionable costs consisting of ineligible ground stabilization costs, unsupported force account labor costs, ineligible force account labor and excessive fringe benefits costs, unsupported costs, and duplicate costs. In addition, the OIG found that improvement was needed in FEMA's procedures for project management and monitoring. (OIG-DS-17-04, July 28, 2004, OA)

Audit of the State of Kentucky Administration of Disaster Assistance Funds

The OIG reviewed the disaster grants management system and practices of the Kentucky Division of Emergency Management (grantee). The objectives of the review were to determine whether the grantee administered the funds according to federal regulations and FEMA guidelines. The grantee: (1) did not submit quarterly Financial Status Reports for the IFG programs; (2) needs to improve in the preparation and submission of Public Assistance quarterly progress reports; (3) was not in compliance with federal requirements and FEMA approved administrative plans for Public Assistance project monitoring, (4) had not established a mechanism to track outstanding IFG checks; (5) did not have adequate procedures for ensuring compliance with the provisions of the Single Audit Act (Public Law 98-502); and (6) needs to improve in the preparation and submission of Hazard Mitigation program plans. (DA-26-04, May 2004, OA)

Audit of the State of Delaware Administrator of Disaster Funds

The OIG reviewed the disaster grants management system and practices of the Delaware Emergency Management Agency (grantee). The objectives of the review were to determine whether the grantee administered the funds according to federal regulations and FEMA guidelines. The grantee: (1) did not document the day-to-day fiscal procedures used to approve, disburse, and account for expenditures of FEMA disaster grant funds; (2) is not verifying or documenting that matching requirements for HM grants are being satisfied; (3) has no policies or procedures requiring that periodic PA or HM sub grantee monitoring visits be made. (DA-32-04, August 2004, OA)

Utah's Compliance with Disaster Assistance Program's Requirements

KPMG, LLC, an independent accounting firm under contract with the OIG, reviewed the disaster grants management system and practices of the State of Utah. This report focuses on the systems and procedures used by the grantee to comply with these regulations, including the Stafford Act and Title 44 of the Code of Federal Regulations.

The OIG's audit addressed three disaster assistance programs: the Public Assistance program, the HM program, and the IFG program. The scope of the audit was limited to one presidential declared disaster. Further, testing was limited to those programs that were open during the period of the OIG's review, October 1, 2001, through September 30, 2002. The federal share of total funds obligated and expended for the audited disaster through September 30, 2002, was $628,672.

The audit concluded that the State of Utah, for the most part, effectively managed FEMA's disaster assistance programs in accordance with federal requirements. However, some weaknesses in internal controls and non-compliance situations were identified. (DD-17-04, September 15, 2004, OA)

Ohio's Compliance With Disaster Assistance Program's Requirements

Foxx & Company, an independent accounting firm under contract with the OIG, completed an audit of the Ohio Emergency Management Agency's administration and management of FEMA disaster assistance grant programs. The overall objective of this audit was to determine the effectiveness of the grantee's administration and management of disaster assistance programs authorized by the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Public Law 93-288, as amended) and applicable federal regulations. On October 30, 2000, the President signed the Disaster Mitigation Act of 2000 (Public Law 106-390). This law was not fully implemented by FEMA at the time of the audit. Although the scope of the audit included a review of costs claimed, a financial audit of those costs was not performed.

The audit included nine major disasters declared by the President between August 1995 and August 2001. The federal share of obligations for the nine disasters was over $109 million. Federal funds claimed through September 30, 2002, were over $102 million.

The audit concluded that the State of Ohio, for the most part, had effectively managed FEMA's disaster assistance programs in accordance with Federal requirements. However, some weaknesses in internal controls and non-compliance situations were identified. (DD-16-04, August 24, 2004, OA)

Montcalm County Drain Commission, Stanton, MI

The OIG audited $4.38 million in FEMA public assistance funds awarded to the Montcalm County Drain Commission, Stanton, Michigan. Montcalm received the award for damages caused by severe storms and straight-line winds that occurred on May 31, 1998.

Montcalm did not account for and expend FEMA funds according to federal regulations and FEMA guidelines. Specifically, Montcalm awarded a non-competitive contract for $4,383,330 that did not comply with federal procurement standards. As a result, fair and open competition did not occur, and Montcalm's claim included $1,037,459 in contractor profits and $76,733 in markups on subcontractor costs that the OIG questioned as unreasonable and excessive. Montcalm also did not justify ineligible cost overruns that exceeded FEMA approved estimates by $2,844,779, and did not account for FEMA funds by project, as required. As a result, FEMA had no assurance that claimed costs were reasonable and within the scope of work defined for the individual projects.

Further, Michigan State Police, Emergency Management Division, the grantee, did not adequately manage its sub grant to Montcalm. The grantee did not: (1) ensure that Montcalm was aware of federal regulations; (2) properly process requests for project time extensions; or (3) provide FEMA with timely and accurate progress reports. As a result, the FEMA Regional Office did not have the information needed to meet its grant oversight responsibilities. (DD-18-04, September 2004, OA)

City of Los Angeles Housing Authority, Los Angeles, California

The Authority received an award of $3.27 million from the California Office of Emergency Services for facilities damaged as a result of the January 1994 Northridge earthquake. The OIG determined that the Authority earned $566,979 of interest income on a $2.9 million FEMA advance, and the interest was not remitted to FEMA as required. In addition, the Authority claimed $59,675 of costs not supported with documentation showing that the charges were for disaster related work. (DS-20-04, September 2004, OA)

World Trade Center Disaster Fraud

The OIG initiated an investigation based on a letter written by the subject to a former Federal Emergency Management Agency (FEMA) director requesting disaster assistance as a result of the World Trade Center attack. In this letter, the subject claimed that his wife was killed in the collapse of Tower One and that his children suffered from the loss

of their mother. Additionally, he requested monetary assistance for property that was damaged when the buildings collapsed. The investigation disclosed that the subject was not married at the time of the attack, did not own the type of vehicle that he claimed was damaged, and had no children. In fact, on September 11, 2001, the subject was in jail in a suburb of Atlanta, Georgia. A federal grand jury indicted him for false statements and three counts of mail fraud. He entered a guilty plea to all four counts and was sentenced to time served. He is currently awaiting deportation to Nigeria and was remanded to the custody of ICE. (OI)

National Flood Insurance Civil Recovery

The OIG initiated a civil investigation as a result of successful criminal prosecution of fraud against the National Flood Insurance Program. At the criminal trial, a contractor and flood insurance adjuster were found guilty of defrauding the program and both are serving time in a federal penitentiary. Subsequent to the criminal prosecutions, the U.S. Attorney's Office, Eastern District of North Carolina, pursued a civil action under the Civil False Claims Act (31 U.S.C. 3729, as amended), against a condominium homeowners' association and its former president. Both parties were aware of the criminal fraud that occurred and received benefit from those actions. The U.S. Attorney's Office negotiated a civil settlement agreement with the homeowners' association, which agreed to pay $600,000 in damages, and the former president of the association, who agreed to pay $300,000 in damages. (OI)

California Freeze (Update)

In February 1999, a disaster was declared by the President for California's Central Valley area as a result of temperatures' dropping below freezing causing extensive damage to the citrus crop. The citrus workers were entitled to a number of FEMA assistance programs based on the loss of income. The OIG identified numerous fraudulent individual assistance applications that caused unwarranted government funds to be distributed to undeserving claimants. Criminal action has been completed in this investigation and, during this reporting period, the remaining two defendants pleaded guilty to identity theft, conspiracy, and illegal use of a social security number. The defendants were sentenced to serve three months in custody followed by three years of supervised release, fined $1,200, and ordered to pay $4,833.87 in restitution. (OI)

Super Typhoon Paka (Update)

In December 1997, a disaster was declared by the President for the Island of Guam due to extensive heavy wind, rain, and flood damage as a result of Super Typhoon Paka. FEMA

funded a $1.2 million dollar project to replace the damaged bus shelters throughout the island with 387 new concrete bus shelters. The Governor of Guam's Chief of Staff awarded the bus shelter contract to a business rival of the Governor, in exchange for his support in the 1998 gubernatorial campaign. The Chief of Staff also gathered fraudulent backdated supporting bids from cooperating contractors to satisfy FEMA requirements. During this reporting period, the former Chief of Staff and a local businessman were indicted on seventeen counts to include bribery, money laundering, bank fraud, conspiracy, and engaging in financial transactions with the proceeds of illegal activity. A January 10, 2005 trial date has been set. (OI)

Iowa Severe Storms (Update)

In May 1999, a disaster was declared by the President in Iowa based on severe storms which included flooding and tornadoes. FEMA funded the disaster relief. A husband and wife filed a claim with FEMA claiming that their home in a certain city in Iowa, was their primary residence in order to be eligible for the available FEMA funding. The investigation proved that this was not their primary residence. The husband and wife were indicted on two federal counts of false statements. They were arrested and pleaded guilty. The husband was sentenced to two years probation and ordered to pay a fine, an assessment fee, and restitution. The wife entered into a one-year pre-trial diversion program. (OI)

American Philanthropy Association (APA) President and Shelter Manager Indicted (Update)

The OIG and the FBI initiated an investigation into the allegation that the President and Shelter Manager of the APA were fraudulently receiving grants from the FEMA Emergency Food & Shelter program. The investigation proved that in 1997 and 1998, the President and Shelter Manager, through APA, received $107,160 in FEMA Emergency and Food Shelter funds by submitting false daily log sheets bearing forged resident signatures. The President and Shelter Manager were indicted on multiple counts of conspiracy, false claims, false statement, and theft of government property. The President of APA has previously pleaded guilty and was sentenced. The Shelter Manager became a fugitive, was arrested, and March 10, 2004, pleaded guilty to the above charges. On June 7, 2004, the Shelter Manager was sentenced to serve 20 months in custody; three years supervised release; fined $100; and, ordered to pay $103,569 in restitution. (OI)

Minnesota Disaster Cleanup Company Indicted

A former disaster cleanup company, that performed work in New York, Wisconsin, and Minnesota, has been indicted for overcharging government agencies and businesses by $1.17 million. A federal grand jury charged the company, its owner and top executives, with false and inflated billing and wire fraud associated with flood reconstruction in Minnesota. The investigation was initiated after officials became suspicious about inflated bills submitted by the company for cleanup work resulting from a tornado that hit Siren Village, Wisconsin in June 2001. This is an "ongoing criminal enterprise" that covered three states. Besides the firm, four Minnesota men, the owner and former president, along with senior executives were indicted. Each person pleaded not guilty. They also face a racketeering charge for conspiring to defraud customers by inflating bills and persuading employees to destroy records to conceal overcharging. Trial is set for January 2005. (OI)

Management

Management Letter for the FY 2003 DHS Financial Statement Audit

As part of the DHS FY 2003 consolidated financial statement audit, the OIG issued a "management letter" identifying certain non-material internal control and operational matters requiring DHS management attention. The independent public accounting firm, KPMG LLP, performed the audit at the OIG's direction and with the OIG's assistance. The management letter contained recommendations to address a variety of issues, including property management, grants management, fee receipt, financial reporting, suspense accounts, and other miscellaneous internal control and operational matters. (OIG-04-042, September 2004, OA)

Inadequate Security Controls Increase Risks to DHS Wireless Networks

DHS has not provided sufficient guidance to its components or established adequate controls necessary to implement its wireless program. Specifically: (1) wireless policy is incomplete, (2) procedures do not establish a sound baseline for wireless security implementation, and (3) the National Wireless Management Office is not exercising its full responsibilities in addressing DHS' wireless technologies. Further, DHS has not established adequate security measures to protect its wireless networks and devices against security risks. Finally, although the DHS security policy requires certification and accreditation (C&A) for its systems to operate, none of the wireless systems reviewed had been certified or accredited. As a result of these wireless network exposures, DHS cannot ensure that the sensitive information processed by its wireless systems is effectively protected from unauthorized accesses or potential misuse.

The OIG's report includes five recommendations that will assist DHS in remedying the deficiencies that the OIG identified. Specifically, the DHS CIO should:

- define the conditions and limitations for using wireless technologies in the DHS security policy.
- update the DHS Information Technology Security Program Handbook for Sensitive Systems (Handbook) to include implementation procedures required by National Institute of Standards and Technology Special Publication 800-48 for the use of wireless technologies.
- require the National Wireless Management Office to provide the necessary oversight and guidance to align components' wireless programs with DHS' wireless goals.
- implement a standardized configuration for wireless technologies on DHS networks.
- complete a C&A for each DHS system.

The DHS CIO agreed with and has already taken steps to implement each of the recommendations. However, the DHS CIO disagreed that the National Wireless Management Office is not exercising its full responsibilities. Based on the OIG's assessment of the CIO's response, the OIG stands by its conclusion that oversight of the wireless functionality within DHS needs to be improved. (OIG-04-027, June 2004, IT)

Evaluation of DHS' Security Program for Its Intelligence Systems

The OIG performed an independent evaluation of DHS' security program for its intelligence systems as required by the Federal Information Security Management Act (FISMA) (Public Law 107-347). The OIG reviewed five systems for compliance with FISMA and Director Central Intelligence Directive 6/3. The OIG also performed vulnerability tests of security controls for these five systems. This review was conducted between April 2004 and July 2004. This report represents a baseline evaluation of DHS' intelligence program according to FISMA. (OIG-04-034, August 2004, IT)

Improvements Needed To DHS' Information Technology Management Structure

The DHS CIO has a significant role to play in guiding IT resources and capabilities to meet the department's diverse missions. The enormous task of creating one network

and one infrastructure to ensure IT connectivity among the department's 22 legacy organizations is daunting. Specifically, some of the CIO's challenges are to implement an enterprise architecture; standardize and integrate the department's many duplicative systems and tools; and institute a program to address the risks and vulnerabilities facing DHS' IT systems.

Despite these key responsibilities, the CIO is not a member of the senior management team with authority to manage department-wide technology assets and programs strategically. There is no formal reporting relationship between the DHS CIO and the CIOs of major component organizations, which hinders department-wide support for the CIO's central IT direction. Further, the CIO has limited staff resources to assist in carrying out the planning, policy formation, and other IT management activities needed to support departmental units. These deficiencies in the IT organizational structure are exemplified by the CIO's lack of oversight and control of all DHS' IT investment decision-making. Instead, there is a reliance on cooperation and coordination within DHS' CIO Council to accomplish department-wide IT integration and consolidation objectives.

DHS would benefit from following the successful examples of other federal agencies in positioning their CIOs to meet federal guidelines. Specifically, repositioning the CIO to report to the Office of the Deputy Secretary would provide the CIO with the authority and influence needed to guide executive decisions concerning department-wide IT investments and strategies. Having component-level CIOs report to both the DHS CIO and their respective agency heads would help ensure commitment to consolidating the IT infrastructure while also meeting business needs. Further, with adequate IT office support and control of all DHS IT investment decision-making processes, the CIO can better ensure successful accomplishment of IT objectives, programs, and initiatives. (OIG-04-030, July 2004, IT)

Management Letter on DHS IT Controls

Information Technology general control weaknesses exist at each bureau across all information technology control areas. Collectively, these weaknesses limit DHS' ability to ensure that critical financial and operational data is maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively affect the internal controls over DHS financial reporting and its operation, and the OIG considers them collectively to represent a material weaknesses under standards established by the American Institute of Certified Public Accountants. A "material weakness" is a condition in which the design or operation of one or more of the internal control components does not reduce, to a relatively low level, the risk that misstatements,

in amounts that would be material in relation to the financial statements being audited, may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions.

A key contributing factor to these issues is the challenge of merging numerous entities into DHS. These various entities have had their own IT functions, controls, and processes. DHS has taken some steps to begin addressing these issues, such as implementing the Information Technology Security Program Publication, which contains many requirements for maintaining a DHS-wide information security program. In addition, DHS is currently designing a department-wide IT architecture, and plans to complete the architecture by the end of FY 2005. Until the architecture is complete and the related IT infrastructure, controls, and processes are implemented, DHS' IT control environment will continue to consist primarily of the IT processes and controls in place at the entities that have been transferred to DHS.

To address these weaknesses DHS needs to design and implement DHS-wide policies and procedures related to IT controls, and to enforce the policies and procedures through the performance of periodic control assessments and audits. There should be a focus on implementing and enforcing a DHS-wide security C&A program, and IT training for administrators and users. Many of the technical issues identified during the OIG's review, such as weak technical security controls and the lack of contingency planning strategies, can be addressed through an effective security C&A program and security training program. (OIG-04-038, September 2004, IT)

Evaluation of DHS' Information Security Program for Fiscal Year 2004

DHS has made significant progress over the last year in developing, managing, and implementing its information security program at the departmental level. DHS' Information Security Program Strategic Plan provides the foundation for an agency-wide, consolidated information security program. In this plan, DHS' CIO and Chief Information Security Officer (CISO) identify eight distinct security program areas. These areas are essential to provide security services that protect the confidentiality, integrity, and availability of information, and to assign accountability for the administration of DHS' networks and computing platforms. The strategic plan also describes the goals and objectives for establishing a dynamic information security organization over the next five years.

The DHS CIO, who has oversight responsibility for DHS' information security program, has delegated to the CISO, as required under FISMA, the authority to establish information security policies and procedures throughout the department. Under this

authority, the CISO developed the Information Security Program Management Plan, which is the CISO's blueprint for managing DHS' information security program. The CISO also developed and issued an Information Security Risk Management Plan, which documents DHS' plan for developing, implementing, and institutionalizing a risk management process in support of its information security program.

Even though DHS has made several improvements in its information security program, the organizational components have not yet fully aligned their respective security programs with DHS' overall policies, procedures, and practices. For example:

- DHS cannot effectively manage its information security program while lacking an accurate and complete system inventory. DHS has begun an effort with an outside contractor to identify and establish an agency-wide system inventory. With the exception of IAIP, most components have made attempts to identify their inventory of programs and systems, including those that are contractor owned or operated.

- Although defined a number of times, Information Systems Security Managers (ISSMs) for five of the nine components (CBP, EP&R, IAIP, S&T, and USSS) contacted the OIG for additional clarification on the definition of programs and systems. This continued lack of understanding by those responsible for identifying required program and system information has hindered DHS' ability to compile a comprehensive system inventory.

- As reported in the OIG's FY 2003 security program evaluation, DHS' organizational components are not ensuring that all IT security weaknesses are included in POA&Ms. Therefore, DHS cannot effectively oversee and measure component-level FISMA metrics.

- FISMA metrics data, captured within Trusted Agent FISMA, is not comprehensively verified. Until this verification is accomplished, DHS cannot rely totally on the information reported by the organizational components in Trusted Agent FISMA, which affects overall security program management.

- Most component-level policies and procedures are in draft, such as those for C&A, and have not been formally approved or communicated to program officials and members of the IT security organizations. For example, only three components (EP&R, ICE, and USCG) have updated their C&A policies to ensure their compliance with MD 4300 and National Institute of Standards and Technology Special Publication 800-37.

The OIG made specific recommendations to assist DHS in the development and implementation of its information systems security program in the OIG's FY 2003 report. While a few of these recommendations were implemented, such as the certification of Trusted Agent FISMA and the reporting of DHS' information systems security program as a material weakness, recommendations related to the tracking and remediation of material weaknesses and completion of a system inventory remain open. The OIG recommends that DHS continue to consider its information systems security program a significant deficiency for FY 2004.

The OIG obtained written comments on a draft of this report from DHS' CIO. DHS generally concurred with the report's recommendations and has already initiated several projects in the latter part of FY 2004 that address some of the recommendations. These include a system inventory project that is working toward a comprehensive inventory of DHS' general support systems and major applications. Similarly, a project to review and verify FISMA metrics data captured within an automated system was recently initiated. These and other activities will continue to be implemented in FY 2005 to improve the communication between the CISO and DHS' components and to increase the accountability of the components. (OIG-04-041 September 2004, IT)

United States Coast Guard (USCG)

FY 2003 Mission Performance, United States Coast Guard

The Homeland Security Act of 2002 requires the OIG annually to assess the Coast Guard's performance of all its missions. The OIG's fiscal year 2003 mission performance audit determined how the level of effort directed toward each mission has changed since September 11, 2001, and identified the consequences resulting from the change in mission emphasis. The Coast Guard faces three major barriers to improving or sustaining its mission performance in FY 2004 and beyond: (1) the lack of a comprehensive and fully defined performance management system; (2) the growing workload and associated demand for experienced and trained Coast Guard personnel; and (3) the deteriorating readiness condition of its aged cutter and aircraft fleets. The OIG recommended that the department and the Coast Guard expedite the review and approval of the Coast Guard's proposals to update the Integrated Deepwater System requirements and its acquisition program baseline. This recommendation will ensure that the deteriorating readiness condition is addressed in the FY 2006 budget formulation, as well as the Future Years Homeland Security Plan for 2007-2011. (OIG-04-043, September 2004, OA)

The Coast Guard works in conjunction with the U.S Customs to stop illegal immigrants from entering the U.S. by sea.

USCGC Sturgeon WPB – 87336, 87-Foot coastal Patrol Boat

OIG auditors board and observe a District 1 marine safety inspection of a ship (from Venezuela) in Boston Harbor.

Re-Engining of the HH-65 Helicopter, United States Coast Guard

At the request of the House Appropriations Homeland Security Subcommittee, the OIG reviewed the Coast Guard's actions to re-engine the HH-65 search and rescue helicopter fleet. HH-65 aircrews have reported (and continue to report) ever increasing numbers of in-flight loss of power mishaps resulting from a failure of the aircraft's fuel delivery system. These mishaps led to the Coast Guard's October 2003 decision to impose operating restrictions on the HH-65. According to the Coast Guard, the operational restrictions were not intended to mitigate the risks of in-flight loss of power mishaps, but to mitigate the safety consequences associated with these mishaps. The operating restrictions also affected the Coast Guard's capability to perform its missions, including search and rescue and other humanitarian-related missions.

On January 15, 2004, the Coast Guard selected Integrated Coast Guard Systems (ICGS)[2] to develop and implement a HH-65 re-engining solution. According to the Coast Guard,

[2] ICGS is the Coast Guard's current Integrated Deepwater System contractor

choosing ICGS to develop and implement the re-engining solution maintained a critical linkage with its Deepwater partner, took advantage of ICGS project management and negotiation capability, and helped avoid competition based litigation. The decision also increased the safety, cost, schedule, and operational risks associated with the project by extended negotiations between ICGS and the Coast Guard and between ICGS and its subcontractors. These extended negotiations have postponed the purchase and the delivery of engines and airframe modification kits, delayed the delivery of the first re-engined HH-65 by more than three months, and deferred delivery of the remaining 94 airframes until November 2007, well beyond the Commandant's 24-month timeline for completing the project. More importantly, the delay will expose HH-65 aircrews to additional in-flight loss of power mishaps and will further extend the operational restrictions placed on the HH-65 fleet.

The latest ICGS re-engining proposal was estimated to cost $294 million, or $40 million more than the Coast Guard estimates it would have cost to perform the re-engining at an aircraft repair and supply center as a government performed project. This is a significant development given the impact that these additional expenditures will have on the Coast Guard's ability to sustain and upgrade its legacy air asset. The OIG also determined the Coast Guard needs to resolve the safety, performance, security, and cost issues associated with the MH-68A leased by its Helicopter Interdiction Tactical Squadron.

The report recommends that the Commandant implement the recommendation made by its Assistant Commandant for Operations in May 2004 to re-assert control over the HH-65 re-engining project and perform the re-engining as a government performed project. The Coast Guard does not concur with this recommendation, its primary rationale being that ICGS minimizes the operational, legal, and contract performance risks associated with the re-engining. The Coast Guard believes that it receives significant benefits from the current ICGS contract that far outweigh the costs of having ICGS manage the project. The OIG does not believe those benefits have been demonstrated in this instance.

The report also recommends that the Coast Guard expedite the replacement of the MH-68A helicopters with re-engined HH-65s equipped with the airborne use of force package of upgrades, acquire and refurbish additional HH-65 aircraft and airframes, and use the savings resulting from the termination of the MH-68A lease to mitigate the impact the re-engining project will have on the maintenance and upgrade of its legacy air assets. The Coast Guard agreed in part with these recommendations, but in all three cases cites a lack of funding as the primary reason for not implementing them. (OIG-04-050, September 2004, OA)

HH-65 on a Search and Rescue Training Mission

HH-65A Conducting HIFR operations with a Coast guard Medium Endurance Cutter

Coast Guard Mishandling of Classified Information

In May 2004, the OIG received allegations that the Coast Guard Investigative Service mishandled classified information that was derived from a joint law enforcement counterintelligence initiative. The OIG investigation determined that Coast Guard failed to adhere to established policies, which resulted in the compromise of classified information and material. The U.S. Attorney's Office declined criminal prosecution in this matter in lieu of administrative remedies. Pursuant to the OIG investigation, the Coast Guard has taken corrective action and implemented improved procedures to ensure the safe handling of sensitive information associated with the law enforcement counterintelligence initiative. (OI)

Coast Guard Reservist Exonerated of Payroll Fraud

A state police officer, who was called to active duty with the USCG on September 12, 2001, was alleged to have defrauded the police department of a substantial amount of supplemental pay benefits. The officer allegedly reported to the department that he was serving in the USCG in the pay grade of an E-4, which made the officer eligible to receive supplement pay benefits. The subject was actually serving as a Chief Warrant Officer Three, which would have made him ineligible for supplemental pay. The investigation established that, in two different documents submitted to the local police department in the weeks immediately after September 11, 2001, the officer's duties with the USCG were identified as that of a Chief Warrant Officer. All benefits to which the officer was not entitled have been repaid to the police department. (OI)

Other OIG Activities

Oversight of Non-DHS Audits

The OIG processed 39 audit reports prepared by non-DHS auditors on DHS programs and activities. The OIG continues to monitor the actions taken to implement the recommendations in those reports. The 39 reports included 21 audits conducted in accordance with Office of Management and Budget (OMB) Circular A-133, Audits of States, Local Governments, and Non-Profit Organizations; and 18 contract audits conducted by the Defense Contract Audit Agency.

Significant Reports Unresolved Over Six Months

Timely resolution of outstanding audit recommendations continues to be a priority. As of this report date, OIG is responsible for monitoring 122 reports that contain recommendations that have been unresolved for more than six months. Of the 122 reports, OIG issued 63 and legacy agencies, including FEMA OIG, issued the remaining 59.

Management decisions have not been made for the following significant reports. Further explanations follow each report.

- Thirty-nine OMB Circular A-133 single audit reports.

  Management is currently reviewing the reports and says that it anticipates resolving the recommendations by March 30, 2005.

- Thirty-nine grant audit reports; of which OIG issued 30 audit reports and FEMA OIG issued 9 audit reports.

  One report, City of Hoisington, KS, DD-02-04, reported on the OIG's audit of $2.26 million in FEMA public assistance funds awarded for tornado related damages that occurred on April 21, 2001. The audit disclosed questioned and unsupported costs related to volunteer credits, contractor labor, unallowable markups, and work not related to the disaster.

  Management is currently reviewing the reports and says that it anticipates resolving the recommendations by March 30, 2005.

- Eight contract audit reports.

  Management is currently reviewing the reports and says that it anticipates resolving the recommendations by March 30, 2005.

Legislative and Regulatory Review

Section 4(a) of the Inspector General Act requires the Inspector General to review existing and proposed legislation and regulations relating to agency programs and operations and to make recommendations concerning their impact. In reviewing regulations and legislative proposals, the primary basis for the OIG's comments are the audit, inspection, investigation, and legislative experience of the OIG. The OIG also

participates in the President's Council on Integrity and Efficiency (PCIE). The PCIE provides a mechanism for commenting on existing and proposed legislation as well as regulations that have a government-wide impact.

In addition, the OIG routinely reviews and comments on DHS management directives that involve either departmental programs or operations, or OIG missions and functions. For example, the OIG commented on a draft management directive concerning DHS' use of procurement transactions other than procurement contracts, grants, or cooperative agreements for research and prototype development. The term for these non-traditional mechanisms is "other transaction" authority. The OIG made several comments and suggestions for strengthening DHS policy, particularly concerning potential misuse of the other transaction authority. In addition, the OIG suggested that DHS better define terms that were ambiguous or not commensurate with the other transaction authority, and clarify provisions for procuring services from traditional contractions. DHS agreed with the suggestions and stated its intent to modify or supplement the draft directive to address the OIG's concerns.

The OIG also commented on a draft management directive on DHS Personal Property Management. The OIG's comments emphasized the importance of several financial accounting and property management issues. In particular, it is important that the property management system be integrated with the accounting system. In addition, the OIG commented on several sections where more specific guidance and procedures should be provided either in the management directive or in implementing guidelines.

Congressional Briefings and Testimony

The OIG continued to be in regular contact with OIG's committees of jurisdiction throughout the reporting period. Meetings and briefings with members and their congressional staff ranged from unclassified discussions relevant to our published reports and meetings to discuss requests for work from specific members, to closed briefings for members and their staff on the final results of OIG's most sensitive work.

The Inspector General testified before Congress four times during this reporting period. The official statements and OIG reports discussed in the testimony are publicly available on the OIG's website: http://www.dhs.gov/dhspublic/display?theme=89.

On April 22, 2004, the Inspector General testified before the House Committee on Transportation and Infrastructure, Subcommittee on Aviation, on the Airport Screener Privatization Pilot Program. Based on work of the OIG, the Inspector General said that there was not a sufficient basis to determine conclusively whether the pilot airport

screeners performed at a level equal to or greater than that of the federal screeners. The Inspector General noted that available data, from limited covert testing, suggested that they performed about the same, which was to say "equally poorly," and the apparent consistency in performance was not unexpected, considering the extraordinary degree of TSA involvement in screening, hiring, deploying, training, and promoting the pilot screeners.

TSA's tight controls over the pilot program restricted flexibility and innovation that the contractors might have employed to perform at a level exceeding that of the federal workforce. As a consequence, the pilot program contractors said that they could not effectively and immediately address problems with high attrition levels, understaffing, excessive overtime, and employee morale.

Additionally, the assessment process prevented the contractor from hiring applicants whom they believed were qualified to be screeners, and the pilot program contractors were restricted in the overall number of screeners they could hire, and in how screeners were trained. Further, the TSA's management and oversight of the pilot program was generally decentralized, and program and operational issues had to be routed through numerous divisions within TSA to be approved.

The Inspector General concluded that pilot programs *can* be a useful tool in exploring innovations and improvements. But the TSA must also develop meaningful performance measures and standards so that both overall performance and the effects of new improvements can be measured and assessed, and contractors must be given the flexibility to determine what works best for their own situations.

On June 23, 2004, the Inspector General testified before the House International Relations Committee on stolen passports and the findings reported in the OIG report, *An Evaluation of the Security Implications of the Visa Waiver Program*. The Inspector General discussed the report's findings, and addressed the threat that stolen passports pose to the visa waiver program and more broadly, national security.

The Visa Waiver Program began as a pilot program in 1986 and evolved into a permanent program in which 27 nations participate. The Inspector General noted in his opening remarks that foremost among the security issues in the program is the widespread theft of blank passports from foreign governments. Additional concerns highlighted by the Inspector General are contained in his formal statement, and can be found on the OIG website.

The Inspector General strongly recommended that visa waiver travelers be added to the US-VISIT program because of the additional screening, identification, and exit control features it offers. The department began to apply US-VISIT to the Visa Waiver Program on September 30.

On July 8, 2004, the Inspector General testified before the Senate Governmental Affairs' Subcommittee on Financial Management, the Budget, and International Security, on the consolidated financial statements of the departments of Defense and Homeland Security. Chairman Peter Fitzgerald noted that (at the time) DHS was the only cabinet department not yet subject to Chief Financial Officer's Act requirements, but is required under the Accountability of Tax Dollars Act to prepare and have audited financial statements.

The Inspector General noted in his opening remarks that since the department's formation it has made noteworthy progress in the integration of legacy agencies and the development of department-wide functions; however, there is still much to be done, including needed improvements in DHS financial operations. The most immediate challenge has been the orderly transition of the financial operations of its inherited components and the development of plans for its own integrated financial management system. Further, DHS was presented with the challenge of preparing its first set of financial statements for audit, and met that challenge under difficult circumstances.

For fiscal year 2004, OMB accelerated the reporting deadline for audited financial statements and the *Performance and Accountability Report* to November 15, two and a half months earlier than last year's deadline. Meeting this date will be a considerable challenge for DHS. Because the FY 2003 *Performance and Accountability Report* was issued in February, DHS had little time to take corrective action on the material weaknesses and reportable conditions reported the previous year before they entered the FY 2004 audit cycle. To the extent that these weaknesses remain, they will continue to make preparation of the financial statements and auditing them more difficult. The accelerated reporting date requires a new audit approach that relies more heavily on internal controls and systems and earlier audit testing.

The Inspector General also addressed issues on DHS contracts management, revenue collection, grants management, and information technology. The entire statement of the Inspector General is posted on the DHS OIG website.

On September 9, 2004, the Inspector General testified before the House Government Reform Committee on the cooperation between the Departments of State and Homeland Security on issues affecting U.S. visa policy, and discussed the findings of the following two OIG reports: *An Evaluation of DHS Activities to Implement Section 428 of the*

Homeland Security Act of 2002, concerning the assignment of Department of Homeland Security personnel called "Visa Security Officers" (VSOs) to Saudi Arabia initially, and eventually to other countries around the world; and the April 2004 OIG report, *An Evaluation of the Security Implications of the Visa Waiver Program,* concerning security implications of the visa waiver program.

In his opening remarks, the Inspector General highlighted what he considered to be the most significant findings in each report.

With regard to the Section 428 report, the Inspector General noted the VSO program can enhance the security of the visa issuance process, but the program as presently constituted is not living up to its potential. The aim of the program is to provide a cadre of full-time DHS personnel with general expertise in law enforcement and/or intelligence and specific expertise in document fraud, interview techniques, and the language and customs of the applicable country to work with Department of State consular officials to ensure that visas are not issued to known or suspected terrorists.

Unfortunately, due to funding, organizational, and managerial problems, the ten officers who are or have been serving in Saudi Arabia as of March 2004, served on a temporary duty basis. Only one of the ten has served for longer than 90 days. The rapid turnover and short tenure hampered their effectiveness.

Further, he noted, DHS had not provided the VSOs with the statutorily and practically requisite training in language, fraud detection, and interview techniques. Only one of the ten officers could read and speak Arabic. Moreover, the VSOs lacked the budgetary, administrative, and logistical support they needed to be fully effective in their jobs.

Additionally, the VSOs spent too much time entering visa applicant data into DHS computers that embassy staff had already inputted into State Department computers, limiting the time they could devote to adding counter-terrorism value to the visa issuance process. Finally, as of March 2004, no thorough examination had yet been made of thousands of visa applications that were submitted and approved before 9/11 to determine whether any of the applicants had any ties to the 9/11 terrorists.

The Inspector General concluded his remarks by stating that, before the program is expanded beyond Saudi Arabia, the report recommendations should be implemented. The reports and testimony may be found on the DHS OIG website.

APPENDICES

Appendix 1 Audit Reports with Questioned Costs

Appendix 1b Audit Reports with Funds Put to Better Use

Appendix 2 Compliance – Resolution of Reports and Recommendations

Appendix 3 Management Reports Issued

Appendix 4 Financial Assistance Audit Reports Issued

Appendix 5 Schedule of Amounts Due and Recovered

Appendix 6 Acronyms

Appendix 7 OIG Headquarters and Field Office Contacts and Locations

Appendix 8 Index to Reporting Requirements

Appendix 1
Audit Reports With Questioned Costs

A. Reports pending management decision at the start of the reporting period	107	128,784,930	42,335,085
B. Reports issued/processed during the reporting period with questioned costs	28	23,497,249	4,165,518
Total Reports (A+B)	135	152,282,179	46,500,603
C. Reports for which a management decision was made during the reporting period	32	3,726,065	876,636
(1) Disallowed costs		3,151,533	876,636
(2) Accepted costs		574,532	0
D. Reports put into appeal status during period	0	0	0
E. Reports pending a management decision at the end of the reporting period	103	148,556,114	45,623,967
F. Reports for which no management decision was made within six months of issuance	103	125,058,865	41,458,449

Notes and Explanations:

"Management Decision" occurs when DHS management informs the OIG of its intended action in response to a recommendation and the OIG determines that the proposed action is acceptable.

"Accepted Costs" are previously questioned costs that have been accepted by DHS management as an allowable cost to a government program. Before acceptance, the OIG must agree with the basis for the management decision.

"Questioned costs" are costs that are not supported by adequate documentation or were incurred in violation of a law, regulation, or other provision governing a grant, cooperative agreement, or contract. DHS is responsible for making management decisions on whether to accept or reject the OIG's findings relating to questioned costs. A management decision to accept the OIG's finding 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 Be Put To Better Use

A. Reports pending management decision at the start of the reporting period[1]	11	46,902,883
B. Reports issued during this reporting period	0	0
Total Reports (A + B)	11	46,902,883
C. Reports for which a management decision was made during the reporting period	1	1,980,165
(1) Value of recommendations agreed to by management		1,980,165
(2) Value of recommendations not agreed to by management		0
D. Reports put into the appeal status during the reporting period	0	0
E. Reports pending a management decision at the end of the reporting period	10	44,922,718
F. Reports for which no management decision was made within six months of issuance	10	44,922,718

Notes and Explanations:

"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.

[1]Includes legacy agency reports for which a management decision has not yet been made.

Appendix 2
Compliance – Resolution Of Reports And Recommendations

MANAGEMENT DECISION IS PENDING

3/31/2004	
Reports open over six months	129
Recommendations open over six months	466
9/30/2004	
Reports open over six months	122
Recommendations open over six months	595

CURRENT INVENTORY

Open reports at the beginning of the period	310
Reports issued this period	102
Reports closed this period	115
Open reports at the end of the period	297

ACTIVE RECOMMENDATIONS

Open recommendations at the beginning of the period	1,719
Recommendations issued this period	268
Recommendations closed this period	466
Open recommendations at the end of the period	1,521

Notes and Explanations:

"Open reports" are those containing one or more recommendations for which a management decision or final action is pending.

"Active recommendations" are recommendations awaiting a management decision of final action.

Appendix 3
Management Reports Issued

	Program Office/Report Subject	Report Number	Date Issued
1.	A Review of the Secure Electronic Network for Travelers Rapid Inspection Program	OIG-04-014	6/04
2.	Audit of the Automated Commercial Environment Secure Data Portal: Security Requirements Need to Be Implemented	OIG-04-022	5/04
3.	Review of Deemed Exports	OIG-04-023	4/04
4.	An Evaluation of the Security Implications of the Visa Waiver Program	OIG-04-026	4/04
5.	Inadequate Security Controls Increase Risks to DHS Wireless Networks	OIG-04-027	6/04
6.	A Review of the Use of Alternative Screening Procedures at an Unnamed Airport	OIG-04-028	7/04
7.	Progress and Challenges in Securing the Nation's Cyberspace	OIG-04-029	7/04
8.	Improvements Needed to DHS' Information Technology Management Structure	OIG-04-030	7/04
9.	DHS Challenges In Consolidating Terrorist Watch List Information	OIG-04-031	8/04
10.	Evaluation of the Federal Air Marshal Service	OIG-04-032	8/04
11.	An Evaluation of DHS Activities to Implement Section 428 of the Homeland Security Act of 2002	OIG-04-033	8/04
12.	Evaluation of DHS' Security Program for Its Intelligence Systems	OIG-04-034	8/04
13.	Audit of the Automated Commercial Environment Secure Data Portal: Management Controls Needed Improvement	OIG-04-035	9/04
14.	Audit of Passenger and Baggage Screening Procedures at Domestic Airports	OIG-04-037	9/04
15.	Management Letter on DHS IT Controls	OIG-04-038	9/04

16.	Effectiveness of Customs and Border Protection's Procedures to Detect Uranium in Two Smuggling Incidents	OIG-04-040	9/04
17.	Evaluation of DHS' Information Security Program for Fiscal Year 2004	OIG-04-041	9/04
18.	Management Letter for the FY 2003 DHS Financial Statement Audit	OIG-04-042	9/04
19.	FY 2003 Mission Performance, United States Coast Guard	OIG-04-043	9/04
20.	Evaluation of TSA's Contract for the Installation and Maintenance of Explosive Detection Equipment at United States Airports	OIG-04-044	9/04
21.	An Evaluation of the Transportation Security Administration's Screener Training and Methods of Testing	OIG-04-045	9/04
22.	Assessment of Expenditures Related to the First Annual Transportation Security Administration Awards Program and Executive Performance Awards	OIG-04-046	9/04
23.	Transportation Security Administration Review of the TSA Passenger and Baggage Screening Pilot Program	OIG-04-047	9/04
24.	Review of TSA Screening Practices in Houston, Texas	OIG-04-048	9/04
25.	The Federal Emergency Management Agency's Individual and Family Grant Program Management at the World Trade Center Disaster	OIG-04-049	9/04
26.	Re-Engining of the HH-65 Helicopter, United States Coast Guard	OIG-04-050	9/04

APPENDIX 4

Financial Assistance Audit Reports Issued

	Report Number	Date Issued	Auditee	Questioned Costs	Unsupported Costs	Funds Put to Better Use
1.	DA-23-04	5/04	Dekalb County, Georgia	$121,014	$64,079	$0
2.	DA-24-04	5/04	Virginia Department of Transportation	$4,433	$0	$0
3.	DA-25-04	5/04	Virginia Department of Transportation	$55,592	$0	$0
4.	DA-26-04	5/04	Audit of the State of Kentucky Administration of Sisaster Assistance Funds	$0	$0	$0
5.	DA-27-04	5/04	Edgecombe County Schools, North Carolina	$0	$0	$0
6.	DA-28-04	6/04	Massachusetts Bay Transit Authority	$467,954	$102,607	$0
7.	DA-29-04	6/04	City of Birmingham, Alabama	$0	$0	$0
8.	DA-30-04	6/04	University of the Virgin Islands	$1,636,774	$0	$0
9.	DA-31-04	8/04	City of Goldsboro, North Carolina	$0	$0	$0
10.	DA-32-04	8/04	Audit of the State of Delaware Administrator of Disaster Funds	$0	$0	$0
11.	DA-33-04	8/04	North Carolina Parks and Recreation	$6,582,560	$98,075	$0
12.	DA-34-04	9/04	Municipality of San Juan, Puerto Rico	$524,462	$509,355	$0
13.	DA-35-04	9/04	City of Macon, Georgia	$114,220	$0	$0
14.	DA-36-04	9/04	Brevard County, Florida	$186,437	$0	$0
15.	DA-37-04	9/04	Brevard County, Florida	$305,318	$145,816	$0
16.	DA-38-04	9/04	Greenville Utilities Commission	$58,223	$0	$0
17.	DD-09-04	6/04	Michigan State Police, Emergency Management Division, Lansing, Michigan	$3,402,632	$2,582,281	$0
18.	DD-10-04	7/04	Wyoming's Compliance with Disaster Assistance Program	$14,852	$0	$0
19.	DD-11-04	7/04	Grant Management: Texas' Compliance with Disaster Assistance Program's Requirements	$153,141	$0	$0

20.	DD-12-04	8/04	Hempstead County, Arkansas	$1,032,043	$404,559	$0
21.	DD-13-04	8/04	Cookson Hills Electric Cooperative Inc.	$209,231	$15,442	$0
22.	DD-14-04	8/04	Minnesota's Compliance with Disaster Assistance Program's Requirements	$0	$0	$0
23.	DD-15-04	8/04	City of St. Peter, MN	$1,524,250	$0	$0
24.	DD-16-04	8/04	Ohio's Compliance with Disaster Assistance Program's Requirements	$50,131	$0	$0
25.	DD-17-04	9/04	Grant Management: Utah's Compliance with Disaster Assistance Program's Requirements	$0	$0	$0
26.	DD-18-04	9/04	Montcalm County Drain Commission, Stanton, MI	$835,644	$0	$0
27.	DS-12-04	5/04	Santa Clarita Health Care Association, Santa Clarita, California	$2,061,248	$89,405	$0
28.	DS-13-04	5/04	County of Marin, San Rafael, California	$0	$0	$0
29.	DS-14-04	5/04	Sonoma County, Santa Rosa, California	$0	$0	$0
30.	DS-15-04	5/04	East Bay Regional Park District, Oakland, California	$0	$0	$0
31.	DS-16-04	7/04	King County, Seattle, Washington	$395,931	$7,781	$0
32.	DS-17-04	7/04	City of Seattle, Washington	$306,949	$27,922	$0
33.	DS-18-04	8/04	Conejo Valley Unified School District, Thousand Oaks, CA	$39,740	$39,740	$0
34.	DS-19-04	8/04	City of Kelso, WA	$2,714,373	$0	$0
35.	DS-20-04	9/04	City of Los Angeles Housing Authority, Los Angeles, CA	$620,687	$53,708	$0
36.	DS-21-04	9/04	Sutter County, Yuba City, CA	$49,828	$5,987	$0
37.	DS-22-04	9/04	County of Yuba, Marysville, CA	$28,932	$18,761	$0
			Total	$23,496,599	$4,165,518	$0

Report Number Acronyms:

DA Disaster, Atlanta

DD Disaster, Dallas

DS Disaster, San Francisco

Appendix 5

Schedule Of Amounts Due And Recovered

	Report Number	Date Issued	Auditee	Amount Due	Recovered Costs
1.	DA-04-04	11/03	Bibb County, Georgia		$13,697
2.	DA-14-04	2/04	South Carolina Department of Transportation		$110,416
3.	DA-15-04	2/04	South Carolina Department of Transportation		$12,853
4.	DA-16-04	2/04	Coastal Electrical Power Association, Bay St. Louis, Mississippi		$27,056
5.	DA-18-04	3/04	City of Raleigh, North Carolina		$17,051
6.	DA-19-04	3/04	City of Raleigh, North Carolina		$40,656
7.	DA-26-03	9/03	New Jersey State Police		$1,238
8.	DA-27-03	9/03	Palm Beach County, Florida		$21,773
9.	DD-08-04	3/04	City of Overland Park, Kansas		$7,023
10.	DD-11-03	8/03	Memorial Hermann Hospital, Houston, Texas		$16,508
11.	DD-16-03	9/03	City of Chicago, Illinois		$392,207
12.	DO-10-03	8/04	Kaiser Foundation Health Plan, Inc.,Los Angeles, California		$32,957
13.	DO-11-03	6/03	City of Napa, California		$23,973
14.	DO-14-03	6/03	California Dept. of Forestry & Fire Protection		$585,792
15.	DO-22-03	9/04	California Dept. of Fish and Game		$9,828
16.	DS-01-04	11/03	City of San Leandro, California		$8,221
17.	DS-03-04	11/03	County of San Mateo California		$209,996

18.	DS-04-04	12/03	City of Marysville, California		$43,298
19.	DS-06-04	1/04	City of Oakland, California		$104,687
20.	DS-09-04	2/04	California Department of Water Resources		$571,699
21.	DS-10-04	2/04	California Department of Corrections		$28,630
22.	DS-11-04	3/04	Alameda County, Hayward, California		$478,667
23.	E-10-02	1/04	Gwunnett County, Georgia		$8,063
24.	E-11-03	1/03	Geneva County, Alabama		$26,232
25.	H-S-15-03	7/99	Al Tru Health Systems		$4,124
26.	OIG-S-29-04	2/04	Port of Seattle, Washington		$12,216
27.	W-01-02	10/01	Humboldt County Department of Public Works		$45,918
28.	W-03-03	11/02	California Department of Forestry and Fire Protection, Sacramento, California		$36,589
29.	W-32-01	9/01	Government of Guam, Department of Military Affairs		$267,289
30.	W-33-01	9/01	Government of Guam, Environmental Protection Agency		$21,982
			Total	**$0**	**$3,180,639**

Report Number Acronyms:

DA	Disaster, Atlanta
DD	Disaster, Dallas
DO	Disaster, Oakland
DS	Disaster, San Francisco
E	Eastern District
H-S	Headquarters FEMA OIG
W	Western District

Appendix 6
Acronyms

ACE	Automated Commercial Environment
APA	American Philanthropy Association
BPA	Border Patrol Agent
BTS	Border and Transportation Security
C&A	Certification and Accreditation
CBP	Bureau of Customs and Border Protection
CIO	Chief Information Officer
CIS	United States Citizenship and Immigration Services
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DVD	Digital Video Disc
eCP	e-Customs Partnership
EP&R	Emergency Preparedness and Response
FAM	Federal Air Marshal
FAMS	Federal Air Marshal Service
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Management Act
FY	Fiscal Year
HM	Hazard Mitigation
HSEM	Homeland Security and Emergency Management
IAIP	Information Analysis and Infrastructure Protection
ICE	United States Immigration and Customs Enforcement
ICGS	Integrated Coast Guard Systems
IFG	Individual and Family Grant
IG	Inspector General
INS	Immigration and Naturalization Service
IRS	Internal Revenue Service

ISP	Office of Inspections, Evaluations, and Special Reviews
IT	Information Technology
LASP	Lost and Stolen Passports
NCSD	National Strategy to Secure Cyberspace
NICB	National Insurance Crime Bureau
OA	Office of Audits
OI	Office of Investigations
OIAPR	Office of Internal Affairs and Program Review
OIG	Office of Inspector General
OMB	Office of Management and Budget
PA	Public Assistance
S&T	Science and Technology
SENTRI	Secure Electronic Network for Travelers Rapid Inspection
SFD	State Forestry Division
TDEM	Texas Division of Emergency Management
TSA	Transportation Security Administration
US-CERT	United States Computer Emergency Readiness Team
USCG	United States Coast Guard
USSS	United States Secret Service
US-VISIT	United States Visitor and Immigrant Status Indicator Technology
VSO	Visa Security Officers
VWP	Visa Waiver Program

Appendix 7
OIG Headquarters and Field Office Contacts

Department of Homeland Security
Attn: Office of Inspector General
Stop: 2600
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

Clark Kent Ervin……. Inspector General
Richard L. Skinner…….. 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, Evaluations, and Special Reviews
Frank Deffer……. Assistant Inspector General/Information Technology
Edward F. Cincinnati……... Assistant Inspector General/Administrative Services
Tamara Faulkner……. Congressional Liaison and Media Affairs
Vacant……..……... Executive Assistant to the Inspector General

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
408 Atlantic Ave., Room 330
Captain J.F. Williams Federal Building
Boston, MA 02110
(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, Room 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 401
Miramar, FL 33027
(954) 602-1980 / Fax: (954) 602-1033

Philadelphia, PA
502D Greentreen Executive Campus
Route #73 and Lincoln Dr.
Marlton, NJ 08053
(856)968-4907 / Fax: (856) 968-4914

San Francisco, CA
1111 Broadway, Suite 1200
Oakland, CA 94607-4052
(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) 294-2530 / Fax: (787) 771-3617

Locations of Investigative Field Offices

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

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., Room 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
109 Shiloh Dr., Suite 430
Laredo, TX 78045
(956) 723-4021 / Fax: (956) 717-6465

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, Room 510
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

Philadelphia, PA
Greentree Executive Campus
5002 Lincoln Drive West, Suite B
Marlton, NJ 08053
(856)968-6600 / Fax: (856) 968-6610

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

San Francisco, CA
1301 Clay St., Suite 420N
Oakland, CA 94612-5217
(510) 637-4311 / Fax: (510) 637-4327

Seattle, WA
1110 3rd Ave., Suite 116
Seattle, WA 98101
(206) 262-2110 / Fax: (206) 262-

St. Thomas, VI
Office 550 Veterans Dr., Room 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
Federal Office Building
10 East Broadway, Suite 105
Tucson, AZ 85701
(520) 670-5243 / Fax: (520) 670-5246

Washington, DC (Washington Field Office)
245 Murray Drive, SW
Building 410
Washington, DC 20528
(202) 254-4096 / Fax: (202) 254-4292

The following field office personnel are temporarily operating out of their regional field office:

- Yuma agents are in El Centro, CA
- Buffalo, Boston,and New York agents are in Marlton, NJ

Appendix 8
Index to Reporting Requirements

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

Requirements	**Page**
Review of Legislation and Regulations	56
Significant Problems, Abuses, and Deficiencies	5-55
Recommendations with Significant Problems	5-55
Prior Recommendations Not Yet Implemented	56
Matters Referred to Prosecutive Authorities	Inside Cover
Summary of Instances Where Information Was Refused	N/A
Listing of Audit Reports	65-68
Summary of Significant Audits	5-55
Reports with Questioned Costs	62, 67--68
Reports Recommending That Funds Be Put To Better Use	63
Summary of Reports in which No Management Decision was Made	56, 62-63
Revised Management Decisions	N/A
Management Decision Disagreeements	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, call the OIG Hotline at 1-800-323-8603; write to Department of Homeland Security, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.