U.S. Department of Justice
Office of the Inspector General

Office of the Inspector General Semiannual Report to Congress

April 1, 2007 – September 30, 2007

Online Report Availability

Many audit, evaluation and inspection, and special reports are available at www.usdoj.gov/oig.

Additional materials are available through the Inspectors General Network at www.ignet.gov.

For additional copies of this report or copies of previous editions, write:

DOJ/OIG/M&P
1425 New York Avenue, NW
Suite 7000
Washington, DC 20530

Or call: (202) 616-4550

Message From the Inspector General

The past 6 months have been busy and eventful for the Office of the Inspector General (OIG). I do not believe our office has ever had as many important and sensitive reviews ongoing at the same time. These reviews include an investigation examining the removal of U.S. attorneys and alleged politicization in the Department of Justice's (Department) hiring process for career employees; a follow-up review of the Federal Bureau of Investigation's (FBI) use of national security letters; a review of the Department's involvement with the National Security Agency (NSA) terrorist surveillance program; and a review of the FBI's involvement in and observations of detainee interrogations in Guantanamo Bay, Iraq, and Afghanistan.

Although the size of our staff has not grown in recent years, our responsibilities have increased significantly. I am proud of the work of OIG staff in professionally handling these assignments, as well as many other important audits, inspections, and investigations. Examples of work completed during this reporting period and that we describe in this semiannual report include a follow-up review of the Terrorist Screening Center, a review of the U.S. Marshals Service's (USMS) efforts to protect the federal judiciary, the third in a series of audits of the FBI's development of its Sentinel information and case management system, an evaluation of coordination efforts among Department violent crime task forces, and an assessment of the FBI's progress in implementing improvements in its internal security practices in response to our 2003 report examining the activities of convicted spy Robert Hanssen. In addition, our Investigations Division continues to handle sensitive criminal and administrative investigations of allegations of misconduct related to the Department's programs and operations.

This semiannual report also includes the OIG's updated list of top management and performance challenges facing the Department. As in past years, the top challenge facing the Department is counterterrorism, and many completed and ongoing OIG reviews focus on that issue. However, this year we also have included on the list the challenge of restoring confidence in the Department and its operations. The Department has faced significant criticism of its actions and has endured a great deal of turmoil during the past several months. These issues, coupled with numerous vacancies in senior positions, create a challenge for the new Attorney General and Department leaders to reestablish public confidence in the Department. We look forward to working with the new Attorney General in this and other areas.

Finally, I again want to express my gratitude to the dedicated OIG employees who work day-in and day-out to fulfill the OIG's important mission. They are talented public servants who deserve recognition for their dedication in their efforts to improve the Department and its operations.

Glenn A. Fine
Inspector General
October 31, 2007

Table of Contents

Highlights of OIG Activities

The following table summarizes OIG activities discussed in this report. As these statistics and the following highlights illustrate, the OIG continues to conduct wide-ranging oversight of Department programs and operations.

Statistical Highlights

April 1, 2007 – September 30, 2007

Allegations Received by the Investigations Division	5,150
Investigations Opened	220
Investigations Closed	197
Arrests	69
Indictments/Informations	76
Convictions/Pleas	39
Administrative Actions	142
Fines/Restitutions/Recoveries	$239,927
Audit Reports Issued	137
Questioned Costs	$22 million
Funds Put to Better Use	$350,000
Recommendations for Management Improvements	330

Examples of OIG audits, evaluations, and special reports completed during this semiannual reporting period include:

- **Follow-up Review of the Terrorist Screening Center.** The OIG completed a follow-up review of the Terrorist Screening Center, a multi-agency effort administered by the FBI to consolidate terrorist watchlists and provide around-the-clock responses for screening individuals. Our follow-up review determined that the Terrorist Screening Center has made improvements since our previous audit was completed in 2005. However, the Center has not ensured that the information in its consolidated database is complete and accurate, its management of the watchlist database continues to have significant weaknesses, and the database continues to lack important safeguards for ensuring data integrity.

- **Judicial Security.** The OIG completed a follow-up review of the USMS's progress in evaluating and responding to threats made against federal judges and other court personnel that the USMS protects. Our follow-up report found that the USMS's efforts to assess reported threats and identify potential threats against the judiciary languished after our initial review was issued in 2004. Our follow-up review found that, more than 2 years after issuance of our 2004 report, the USMS still had a backlog of 1,190 threat assessments. However, during our follow-up review the USMS assigned additional resources to address the backlog and as a result the backlog has been eliminated. We also found that the USMS has made only limited progress with its Office of Protective Intelligence program, which was established, in part, to provide a centralized unit to proactively identify potential threats, because additional resources primarily were assigned to reduce the backlog of pending threats and assess new threats rather than proactively identify potential threats. We

determined that the USMS has successfully implemented a home alarm program for federal judges and has begun enhancing its Technical Operations Group to provide sophisticated technological support for judicial security investigations and intelligence work. The USMS concurred with most of our recommendations.

- **Coordination of Violent Crime Task Force Investigations.** An OIG review of the coordination efforts among four of the Department's violent crime task forces determined that the Department did not adequately coordinate the operations of its violent crime task forces to prevent duplication of effort. However, we found that task forces in four of the eight cities we visited were better coordinated because the U.S. attorneys and local task force managers there implemented local policies on coordination, and the task forces used information-sharing systems to coordinate their operations. The Department agreed with our recommendations and has since required each component to certify that it has adopted a policy requiring the use of information-sharing and deconfliction measures to coordinate investigations in areas where more than one violent crime task force operates. The Department also directed U.S. attorneys to report to the Department on violent crime task force coordination efforts, the nature of any coordination problems identified, and guidance or policies adopted or revised to address problems.

- **Hanssen Report Recommendations.** The OIG issued a follow-up report examining the FBI's progress in responding to recommendations made in our August 2003 review of the FBI's handling of Robert Hanssen, the most damaging FBI spy in U.S. history. Our 2003 review concluded that Hanssen escaped detection because of long-standing systemic problems in the FBI's counterintelligence program and a deeply flawed internal security program. Our follow-up report found that, while the FBI has made significant progress in implementing most of our recommendations, it has not fully implemented several critical recommendations and its progress in several other areas has been mixed. The OIG's current report found that the FBI agreed to dedicate a new unit exclusively to determining whether the FBI has been penetrated and to fill a senior operational position in its Counterespionage Section with a representative from the Intelligence Community. However, the FBI still has not fully implemented several critical internal security recommendations. For example, we determined that the FBI has not established a central repository to receive, collect, store, and analyze derogatory information concerning FBI employees, and its progress in improving its background reinvestigation program has been mixed. The FBI agreed to implement both previous and new OIG recommendations.

- **Sentinel III: Status of the FBI's Development of its Case Management System.** The OIG's third audit examining the FBI's ongoing development of its Sentinel case management project determined that the FBI has implemented several management controls and processes designed to help it adequately manage the development of Sentinel and bring it to a successful conclusion. We also found that the FBI has made progress addressing most of the concerns we identified in our two previous audits. However, we concluded that the FBI must make additional progress in certain areas, such as the implementation of its earned value management system and risk management. Our report contained nine new recommendations to help ensure the success of the Sentinel project. The FBI agreed with the recommendations.

- **The Department's Reporting Procedures for Loss of Sensitive Electronic Information.** The OIG examined the processes components must follow when reporting computer security incidents, identifying loss of sensitive electronic information, and notifying individuals whose personally identifiable information may have been lost. When reviewing the policies and procedures for reporting loss of sensitive information at nine Department components, we found that the components did not always report computer security or personally identifiable information incidents within timeframes required by Department and Office of Management and Budget (OMB) standards. We also determined that neither the Department nor any of the components we reviewed have procedures for notifying individuals who could be affected by a loss of personally identifiable information. We made eight recommendations to help the Department and its components improve procedures for responding to the loss of sensitive electronic information. The Department concurred with our recommendations.

Investigations

As shown in the statistics in the table at the beginning of this section, the OIG investigates many allegations of misconduct involving Department employees or contractors hired with Department money. Examples of the OIG's investigations discussed in this semiannual report include:

- An OIG investigation led to the arrest of 11 Federal Bureau of Prisons (BOP) correctional officers charged with violating the civil rights of 2 inmates at the BOP Metropolitan Detention Center in Brooklyn, New York. According to indictments issued in the Eastern District of New York, five correctional officers participated in a planned beating of an inmate and then attempted to disguise the attack by claiming in written reports that the inmate became combative as they attempted to prevent him from committing suicide. In a separate incident, five correctional officers, including one who participated in the previously described attack, physically assaulted an inmate in an elevator while escorting him to a special housing unit within the facility. These five correctional officers and two additional officers also were charged with writing false reports concerning this incident. Several of the defendants pled guilty to these offenses, and trials on the remaining defendants are upcoming.

- An investigation by the OIG's Los Angeles Field Office determined that a BOP correctional officer accepted $10,000 in bribes in exchange for smuggling contraband into the Federal Correctional Complex in Lompoc, California, and a second correctional officer met with an undercover agent and accepted 5 ounces of black tar heroin, an iPod, and a $7,500 bribe in exchange for smuggling contraband into the institution. Both correctional officers were charged with bribery and introduction of contraband. The first correctional officer was sentenced to 18 months' incarceration followed by 24 months' supervised release. The second correctional officer was sentenced to 30 months' incarceration followed by 24 months' supervised release.

- An OIG investigation determined that a deputy U.S. marshal accepted multiple bribes totaling approximately $6,000 from a confidential informant in exchange for providing sensitive law enforcement information to the informant on numerous occasions. The deputy U.S. marshal resigned from his position as a result of our investigation. Sentencing is pending.

- An OIG investigation determined that a Law Enforcement Coordinating Committee liaison in the U.S. Attorneys' Office (USAO) in the Southern District of Alabama obtained sensitive information on a federal grand jury investigation and provided that information to unauthorized persons. The liaison pled guilty to theft of public property.

Ongoing Work

This report also describes ongoing OIG reviews of important issues throughout the Department, including:

- Follow-up review of the FBI's use of national security letters and Section 215 orders
- Review of the FBI's involvement in and observations of detainee interrogations in Guantanamo Bay, Iraq, and Afghanistan
- The Department's removal of U.S. attorneys and alleged politicization in the hiring of Department career employees
- Review of the Department's involvement with the NSA's Terrorist Surveillance Program
- Review of the Department's watchlist nomination process
- The FBI's efforts to resolve terrorist threats and suspicious incidents
- The FBI's efforts to combat crimes against children
- The BOP's efforts to manage inmate health care
- Reviews of ATF's and the Drug Enforcement Administration's (DEA) controls over weapons, laptops, and other sensitive property
- The Department's Victim Notification System

OIG Profile

The OIG is a statutorily created, independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct involving Department programs and personnel and promote economy and efficiency in Department operations. The OIG investigates alleged violations of criminal and civil laws, regulations, and ethical standards arising from the conduct of Department employees in their numerous and diverse activities. The OIG also audits and inspects Department programs and assists management in promoting integrity, economy, efficiency, and effectiveness. The OIG has jurisdiction to review the programs and personnel of the FBI, USMS, DEA, BOP, ATF, USAO, and all other organizations within the Department, as well as contractors of the Department and organizations receiving grant money from the Department.

The OIG consists of the Immediate Office of the Inspector General and the following divisions and office:

- **Audit Division** is responsible for independent audits of Department programs, computer systems, and financial statements. The Audit Division has field offices in Atlanta, Chicago, Dallas, Denver, Philadelphia, San Francisco, and Washington, D.C. Its Financial Statement Audit Office and Computer Security and Information Technology Audit Office are located in Washington, D.C. Audit Headquarters consists of the immediate office of the Assistant Inspector General for Audit, the Office of Operations, the Office of Policy and Planning, and an Advanced Audit Techniques Group.

- **Investigations Division** is responsible for investigating allegations of bribery, fraud, abuse, civil rights violations, and violations of other criminal laws and administrative procedures governing Department employees, contractors, and grantees. The Investigations Division has field offices in Chicago, Dallas, Denver, Los Angeles, Miami, New York, and Washington, D.C. The Fraud Detection Office is located in Washington, D.C. The Investigations Division has smaller, area offices in Atlanta, Boston, Detroit, El Paso, Houston, Philadelphia, San Francisco, and Tucson. Investigations Headquarters in Washington, D.C., consists of the immediate office of the Assistant Inspector General for Investigations and the following branches: Operations, Special Operations, Investigative Support, Research and Analysis, and Administrative Support.

- **Evaluation and Inspections Division** conducts program and management reviews that involve on-site inspection, statistical analysis, and other techniques to review Department programs and activities and makes recommendations for improvement.

- **Oversight and Review Division** blends the skills of attorneys, investigators, program analysts, and paralegals to review Department programs and investigate sensitive allegations involving Department employees and operations.

- **Management and Planning Division** provides advice to OIG senior leadership on administrative and fiscal policy and assists OIG

components in the areas of budget formulation and execution, security, personnel, training, travel, procurement, property management, information technology, computer network communications, telecommunications, quality assurance, internal controls, and general support.

- **Office of General Counsel** provides legal advice to OIG management and staff. It also drafts memoranda on issues of law; prepares administrative subpoenas; represents the OIG in personnel, contractual, and legal matters; and responds to *Freedom of Information Act* requests.

The OIG has a nationwide workforce of approximately 400 special agents, auditors, inspectors, attorneys, and support staff. For fiscal year (FY) 2007, the OIG's direct appropriation was $71 million, and the OIG received an additional $3.5 million in reimbursements.

As required by Section 5 of the *Inspector General Act of 1978* (IG Act), as amended, this *Semiannual Report to Congress* reviewing the accomplishments of the OIG for the 6-month period of April 1, 2007, through September 30, 2007, is to be submitted no later than October 31, 2007, to the Attorney General for his review. The Attorney General is required to forward the report to Congress no later than November 30, 2007, along with information on the Department's position on audit resolution and follow-up activity in response to matters discussed in this report.

Additional information about the OIG and full-text versions of many of its reports are available at www.usdoj.gov/oig.

Multicomponent Audits, Reviews, and Investigations

While many of the OIG's audits, reviews, and investigations are specific to a particular component of the Department, other work spans more than one component and, in some instances, extends to Department contractors and grant recipients. The following describes OIG audits, reviews, and investigations that involve more than one Department component.

Reports Issued

Coordination of Violent Crime Task Force Investigations

At the request of the Senate Appropriations Committee, the OIG's Evaluation and Inspections Division reviewed the coordination efforts among four of the Department's violent crime task forces: ATF's Violent Crime Impact Teams, DEA's Mobile Enforcement Teams, FBI's Safe Streets Task Forces, and USMS's Regional Fugitive Task Forces. The need to coordinate task force operations has grown because of the increasing number of cities with multiple Department task forces.

Overall, we found that the Department has not adequately coordinated the operations of its violent crime task forces to prevent duplication of effort, particularly when the Department created new task forces in jurisdictions in which other task forces already were operating. Although the missions of these task forces overlap, the Department had not required components to coordinate operations or investigations, cooperate in joint investigations, or deconflict law enforcement events. The one exception was the violent crime task forces that were focused on gang crime. In August 2005, the Department issued a policy requiring components to obtain the Deputy Attorney General's approval to conduct anti-gang programs and activities in new locations. However, that policy has not been applied to other types of violent crime task forces.

During field visits in eight cities with multiple task forces, the OIG determined that task forces in four cities were better coordinated because the U.S. attorneys and local task force managers there implemented local policies on coordination, and the task forces used information-sharing systems to coordinate their operations. In the other four cities, the task forces operated as independent entities rather than as part of a coordinated Department approach for combating violent crime. In these cities we found less coordination and more instances of duplicate investigations. We also found that failure to coordinate task force investigations resulted in three "blue-on-blue" incidents in which task force members and informants were targeted as criminals by other task forces. We concluded that guidance was needed to address the problem of competition for state and local law enforcement resources among the Department's four violent crime task forces. Several special agents in charge,

U.S. marshals, and task force managers stated that the participation of local officers was critical to the success of their task forces.

The OIG made four recommendations to improve the coordination of the Department's violent crime task forces, including that the Department implement guidance for coordinating task force operations and require each of the task forces to use national and local information-sharing and deconfliction systems to coordinate investigations and protect officer safety. The Department concurred with the four recommendations and has since required each component to certify that it has adopted a policy requiring the use of information-sharing and deconfliction measures to coordinate investigations in areas where more than one violent crime task force operates. The Department also directed U.S. attorneys to report to the Department on violent crime task force coordination efforts, the nature of any coordination problems identified, and guidance or policies adopted or revised to address problems.

The Department's Reporting Procedures for Loss of Sensitive Electronic Information

In June 2007, the OIG's Evaluation and Inspections Division released a report that examined the process Department components must follow when reporting computer security incidents, identifying losses of sensitive electronic information, and notifying individuals whose personally identifiable information may have been lost. Throughout the federal government personally identifiable information, including social security numbers, medical histories, and tax information, has been compromised after computers or storage media have been lost or stolen.

We reviewed the policies and procedures for reporting loss of sensitive information at nine Department components that accounted for the majority of computer security incidents reported in the Department. We found that the components implemented policies and procedures required by the Department's Office of the Chief Information Officer to comply with standards set by OMB. However, the components were not always reporting computer security incidents within the timeframes required by the standards. In July 2006, OMB established a new requirement that all federal agencies report incidents involving loss of personally identifiable information within 1 hour of discovery. We found that two of the nine components have not updated their policies and procedures to include the new OMB requirement.

In addition, our analysis of 199 computer security incidents in the Department from July 2006 through November 2006 showed that components were not consistently reporting personally identifiable information incidents within 1 hour of discovery to the Department's Computer Emergency Readiness Team (DOJCERT), as required by as required by the components' Incident Response Plans. Moreover, none of the incidents were reported within 1 hour, as OMB requires, to the U.S. Computer Emergency Readiness Team (US-CERT).

We made eight recommendations to help the Department and its components improve procedures for responding to the loss of sensitive electronic information. The Department concurred with all of the recommendations and has begun implementing corrective actions, including clarifying how quickly computer security incidents must be reported, instructing components on proper reporting of incidents involving classified information, developing reporting measures to ensure that all components meet established timeframes, and developing

procedures for notifying individuals affected by a loss of personally identifiable information.

Civil Rights and Civil Liberties Complaints

Section 1001 of the *USA Patriot Act* directs the OIG to receive and review complaints of civil rights and civil liberties abuses by Department employees, to publicize how people can contact the OIG to file a complaint, and to submit a semiannual report to Congress discussing our implementation of these responsibilities. In August 2007, the OIG issued its 11th report summarizing its Section 1001 activities during the period from January 1, 2007, to June 30, 2007.

The report described the number of complaints we received under this section, the cases that were opened for investigation, and the status of these cases. In addition, the report summarized the results of two OIG reviews that were required by the Patriot Reauthorization Act: a review of the FBI's use of national security letters and a review of the FBI's use of Section 215 orders for business records. Both reports were issued in March 2007, as required by the Patriot Reauthorization Act. As discussed previously in this semiannual report, the OIG is continuing its review of the FBI's use of national security letters and Section 215 orders for business records.

The report also highlighted the resolution of the final OIG recommendation made in our June 2003 report that reviewed the treatment of aliens held on immigration charges in connection with the investigation of the September 11, 2001, terrorism attacks. The one recommendation that remained open called for the FBI and the Department of Homeland Security (DHS) to enter into a memorandum of understanding to formalize policies, responsibilities, and procedures to manage a national emergency involving alien detainees. The DHS and the FBI signed a memorandum of understanding that became effective on June 7, 2007, which addressed the handling of administrative cases involving aliens of national security interest.

Grant Fraud Initiative

Grants represent a significant expenditure of federal funds in a wide variety of federal agencies, including the Department. In 2006, the Department organized the National Procurement Fraud Task Force, which seeks to prevent, detect, and prosecute procurement and grant fraud. As part of that effort, the OIG is chairing the Grant Fraud Committee of the task force.

The Grant Fraud Committee is focusing on three areas to help improve the ability of the federal government to prevent, detect, investigate, and prosecute grant fraud: 1) examining ways to enhance information sharing concerning cases and issues related to grant fraud; 2) coordinating efforts to provide training to auditors, agents, and prosecutors on detecting, investigating, and prosecuting grant fraud; and 3) conducting outreach to agency program managers who manage federal grant programs and grantees to coordinate prevention, detection, and investigation of grant fraud and to communicate best practices in these areas.

In conjunction with its work on behalf of the Grant Fraud Committee, the OIG has implemented a Grant Fraud Initiative to focus on grant issues within the Department. As part of this initiative, the OIG's Audit Division has developed a survey program that examines the internal controls of entities receiving Department grant funds in order to quickly assess the risk

of fraud by those entities. Internal controls are intended to provide reasonable assurance that program goals and objectives are met, resources are adequately safeguarded and efficiently used, and reliable data is maintained and fairly disclosed.

Since March 2007, the OIG has performed approximately 20 of these surveys. In instances where we found that a grantee either did not have sufficient internal controls or did not follow its existing internal controls, we reported that lack of internal controls to the grantee for improvement and to the Department to increase its grantee monitoring and carefully scrutinize any future grant requests from the organization. In addition, the survey findings resulted in several referrals to the OIG's Investigations Division where the grantee had significant internal control deficiencies that raised the risk of fraud. Several of those referrals resulted in fraud investigations, which currently are ongoing. We also found one instance of fraud in grant funds received from another federal agency. We made the appropriate referrals, and that matter is under investigation.

Audit of the Department's Conference Expenditures

The OIG's Audit Division issued a report, undertaken at the request of the Senate Appropriations Committee, which examined the nine most expensive Department conferences held in the United States and the most expensive international conference held between October 2004 and September 2006.

We determined that Department conference sponsors adequately justified reasons to hold the conferences, but inconsistently performed and documented cost comparisons among potential sites. In addition, the Department did not maintain a single financial system capable of providing the actual costs of Department conferences. As a result, when asked to provide conference expenditures to Congress, some Department components reported budgeted, awarded, and estimated conference costs instead of actual expenses, while others did not uniformly include travel or personnel costs.

Our audit found that the cost for some meals and receptions at the conferences were extravagant. For example, a 2005 Office Justice Programs (OJP) Weed and Seed National Conference held in Los Angeles, California, which was attended by 1,500 people, included a $53 per person lunch for 120 attendees; a 1-hour, $64,000 themed "networking" reception; and a post-conference meeting for 30 Department employees who were provided a sandwich buffet lunch at a cost of $44 per person and a themed snack for an additional $25 per person. Overall, this conference's daily food expenses averaged $64 per registrant, which exceeded the approved federal per diem rate of $51 for meals. The 2006 Office of Community Oriented Policing Services (COPS) National Conference in Washington, D.C., which hosted 1,100 attendees, included daily breakfast buffets; two lunches; two themed breaks; and a networking reception that cost $60,000 by itself and included chef-carved roast beef and turkey, a penne pasta station, and platters of Swedish meatballs at a cost of nearly $5 per meatball. The average food and beverage cost per day for the COPS conference was $83 per attendee, $19 over the $64 federal per diem meal rate for Washington, D.C.

In addition, our review of 253 travel vouchers submitted by federal employees who attended the conferences found that 75 percent of these vouchers failed to deduct one or more meals provided at the conferences, as required by federal travel regulations. When federal attendees do not deduct meals provided at government expense, and when component managers do not

systematically review vouchers to ensure that such deductions are made, the government effectively pays for the meals twice.

The OIG made 14 recommendations to the Department regarding conference expenditures, including to: 1) ensure that conference planners compare multiple sites in multiple cities, unless components document an overriding operational reason to hold the conference in a particular city; 2) develop and implement conference food and beverages policies; 3) evaluate how components solicit and hire event planners, since no single entity monitors conference costs to ensure that they are appropriate or that event planners offer the best value for the fees charged; and 4) instruct Department component Chief Financial Officers to adopt procedures confirming that employees deduct appropriate amounts from vouchers for government-provided meals. The Department agreed with all of our recommendations.

Audits of the Department's Major IT Systems

During this semiannual period, the OIG's Audit Division, responding to a request from the House and Senate Appropriations Committees, completed the last of three reports on the Department's major information technology (IT) systems. The first report, issued in March 2006, provided an inventory of Department IT systems. The second report examined the Department's efficiency in tracking costs associated with its most expensive IT systems. For this report, the OIG collected information on 38 major Department IT systems that cost a reported $5.7 billion through FY 2005. We found that the Department's Chief Information Officer and component Chief Information Officers were unable to readily verify the costs reported to them by Department IT system managers, and the Department's various financial systems were not designed to identify and compile costs related to individual IT systems. As a result, IT system cost reporting was fragmented, and individual IT system managers relied on various methods to track costs. Consequently, the costs routinely reported to OMB and Congress were unverified.

As part of the audit, the OIG tested the validity of costs reported by system mangers for 3 of the Department's 38 major IT systems: the FBI's Law Enforcement Online system, DEA's Concorde system, and Justice Management Division's (JMD) Justice Consolidated Office Network. The system managers reported that the 3 systems cost $328 million, but we determined that the costs were understated by at least $68 million. To improve cost reporting for IT systems, the OIG recommended that the Department develop cost reporting methodologies, report IT system costs to OMB consistently in budget and other documents, and consider whether the Department's new financial system can be used to accurately identify the costs of individual IT systems. The Department concurred with our recommendations.

Our third report examined the research, plans, studies, and evaluations that the Department has conducted on its 38 major IT systems and sought to identify the depth and scope of problems the Department has experienced in the formulation of its IT plans. We identified nearly 500 studies, plans, and evaluations that the Department has produced, but found significant gaps between the documents described as necessary in guidelines and those actually prepared for individual projects. We also found a lack of compliance in the areas of systems engineering management, configuration management, quality assurance, validation and verification, and training plans.

Prior OIG reports identified planning problems on individual systems and projects, such as

weaknesses in business process re-engineering, requirements planning, cooperation between agencies, and IT program and contract management. These weaknesses have contributed to project re-starts, cost increases, and delays in the FBI's implementation of a case management system; the termination of the FBI's Laboratory Information Management System project; delays in implementing an interoperable fingerprint identification system that can be used by both the Department and federal immigration authorities; and data integrity problems in the TSC database. Finally, we found that the Department did not produce project management evaluations for either successful or failed IT projects, with the exception of two terminated projects in the FBI.

We recommended that the Department evaluate why project teams do not prepare certain plans and evaluations; reassess the utility of those documents; and consider revising the standards for producing IT studies, plans, and evaluations for individual IT projects. The Department agreed with our recommendations.

Federal Information Security Management Act Audits

The *Federal Information Security Management Act* (FISMA) requires the Inspector General for each agency to perform an annual independent evaluation of the agency's information security programs and practices. The evaluation includes testing the effectiveness of information security policies, procedures, and practices of a representative subset of agency systems. To oversee the implementation of policies and practices relating to information security, OMB has issued guidance to agencies for their FISMA requirements.

For FY 2007, the OIG reviewed the security programs of four Department components: the FBI, USMS, BOP, and JMD. Within these components, we selected for review four sensitive but unclassified systems: the FBI's Combined DNA Index System (CODIS), USMS's Warrant Information Network, JMD's Civil Applicant System, and BOP's Hires/Careers. In addition, we selected one FBI classified system for review.

Based on our FISMA reviews, we responded to the OMB questionnaire by providing updated information about the overall effectiveness of the Department's IT security program. Our review disclosed that the Department had ensured that systems within the FBI, USMS, BOP, and JMD all were certified and accredited, system security controls were tested and evaluated within the past year, and system contingency plans were tested in accordance with FISMA policy and guidance. The OIG also reviewed documented policies and procedures for reporting incidents internally to US-CERT and to law enforcement. Our review found that three (the FBI, BOP, and JMD) of the four components followed documented policies and procedures for reporting incidents internally. However, the OIG obtained incident reports from the USMS for the period September 1, 2006, through July 15, 2007, and identified incidents that were not reported within the Department's required 1 hour timeframe.

Ongoing Work

The Removal of U.S. Attorneys and Hiring for Career Positions

The OIG and the Department's Office of Professional Responsibility are conducting a joint review of the Department's removal of several U.S. attorneys. The joint review also is investigating allegations that Department personnel used political considerations in assessing candidates for career Department

positions. In addition, the joint review is examining hiring for the Department's entry-level Honors Program and Summer Law Intern Program and whether Department employees improperly considered applicants' political affiliations when deciding who to hire for the programs from 2002 through 2006.

Review of the Department's Involvement with the Terrorist Surveillance Program

The OIG is reviewing the Department's involvement with the National Security Agency program known as the "terrorist surveillance program" or "warrantless surveillance program." This review is examining the Department's controls over and use of information related to the program and the Department's compliance with legal requirements governing the program.

The Department's Watchlist Nomination Process

The OIG is auditing the processes used throughout the Department for nominating individuals to the consolidated terrorism watchlist, which is maintained by the Terrorist Screening Center.

The Department's Victim Notification System

In October 2001, the federal government deployed the automated Victim Notification System, which allows victims or potential victims of federal crimes to be notified upon a change in the status of the case in which they are involved – from the investigative, prosecution, incarceration, or release phases. The OIG is reviewing the Victim Notification System to determine if services are being provided as required by the terms of the contract; if the Victim Notification System is an effective tool for government users and victims of crime; if outreach is being performed to encourage participation and information sharing; and if information in the system is accurate.

The Department's Key Performance Indicators

Key Indicators are reported each year within the Department's Performance and Accountability Report and link to the Department's Strategic Plan. The OIG is auditing Key Indicators in Department components to examine whether the data underlying the Key Indicators are complete and accurate.

The Department's Financial Statement Audits

The *Chief Financial Officers Act of 1990* and the *Government Management Reform Act of 1994* require annual financial statement audits of the Department. The OIG oversees and issues financial statement audit reports based on the work performed by independent public accountants. The FY 2007 financial statement audit currently is in process. The results will be included in the Department's FY 2007 Performance and Accountability Report, which is expected to be issued by November 15, 2007.

Federal Bureau of Investigation

The FBI investigates counterterrorism, foreign counterintelligence, civil rights violations, organized crime, violent crime, financial crime, and other violations of federal law. FBI Headquarters in Washington, D.C., coordinates the activities of approximately 29,500 employees in 56 domestic field offices, approximately 400 satellite offices, and 59 foreign liaison posts that work abroad on criminal matters within the FBI's jurisdiction.

Reports Issued

Follow-up Review of the Terrorist Screening Center

The OIG's Audit Division completed a follow-up review of its 2005 audit of the Terrorist Screening Center (TSC), a multi-agency effort administered by the FBI to consolidate terrorist watchlists and provide 24-hour, 7-day a week responses for screening individuals. The follow-up audit concluded that the TSC has made improvements since our previous audit was completed, but weaknesses still existed in several watchlist processes and significant deficiencies remained in the data contained in the consolidated terrorist watchlist.

Since its creation in 2003, the TSC has made significant strides in becoming the government's single point-of-contact for law enforcement authorities requesting assistance in identifying individuals with possible ties to terrorism. Our follow-up audit found that, since our 2005 review, the TSC enhanced its efforts to ensure the quality of watchlist data, increased staff assigned to data quality management, and developed a process and a separate office to address complaints filed by persons who said they were mistakenly included on the terrorist watchlist.

Yet, we also found that the TSC's management of the watchlist database continued to have significant weaknesses. For example, the TSC is developing an upgraded database, but currently maintains two interconnected versions of the watchlist that are not identical and contain differing numbers of records. Our audit also identified 20 watchlist records on suspected or known terrorists that were not made available to the frontline screening agents, such as border patrol officers, visa application reviewers, or local police officers, for use during watchlist screening encounters, such as border crossings, visa processing, and routine traffic stops.

We also concluded that the TSC needed to further improve its efforts for ensuring the accuracy of the watchlist records. We found that, in general, the TSC's actions to review records as part of

its special projects, such as the special review of the Transportation Security Administration's No Fly list, successfully improved the quality of the watchlist data. In contrast, our examination of 105 records subject to routine quality assurance reviews by the TSC found that 38 percent of the records we tested contained errors or inconsistencies that were not identified through the TSC's routine quality assurance efforts.

The OIG also expressed concern that the TSC's ongoing quality assurance review of the watchlist will take longer than projected. In April 2007, during our audit, the TSC continued to conduct a record-by-record review of the consolidated watchlist and anticipated that all watchlist records would be reviewed by the end of 2007. However, the watchlist database has increased by more than 20,000 records per month and contained over 700,000 records as of April 2007. Given this growth and the time it takes for the TSC's quality assurance process, the TSC is underestimating the time required to sufficiently review all watchlist records for accuracy.

The OIG made 18 recommendations to help the FBI improve TSC operations and the quality of its watchlist data, including incorporating elements from the TSC's special project quality assurance reviews to its routine quality assurance review process, developing comprehensive standard operating procedures for quality assurance procedures, and resolving weaknesses in the watchlist data. The FBI agreed with the recommendations and reported that the TSC has begun taking corrective action.

Follow-up Review Examining Hanssen Review Recommendations

The OIG's Oversight and Review Division issued a follow-up report examining the FBI's progress in responding to recommendations made in the OIG's August 2003 review of the FBI's handling of Robert Hanssen, the most damaging FBI spy in U.S. history. Over a 20-year period, Hanssen compromised some of the country's most important intelligence and military secrets, including the identities of dozens of human sources, at least three of whom subsequently were executed. Hanssen pled guilty to espionage charges and was sentenced to life imprisonment in May 2002.

Our 2003 review concluded that Hanssen escaped detection because of long-standing systemic problems in the FBI's counterintelligence program and a deeply flawed internal security program. We made 21 recommendations to help improve the FBI's internal security and its ability to deter and detect espionage.

Our follow-up report found that the FBI has made significant progress implementing most of our recommendations, such as enhancing its coordination with the Department on counterintelligence investigations; improving source recruitment, security, and handling; and addressing various security deficiencies in FBI policies and practices identified in the original Hanssen report. However, the FBI still has not fully implemented several critical recommendations, and its progress in other areas has been uneven and requires further attention. For example, we determined that the FBI has not established a central repository to receive, collect, store, and analyze derogatory information concerning FBI employees. Similarly, the FBI's progress in implementing the OIG recommendation to improve its background reinvestigation program has been mixed.

We also found that, despite its response to our original report, the recent conviction of FBI intelligence analyst Leandro Aragoncillo on espionage-related charges revealed mixed

progress in the FBI's actual implementation of our recommendations as well as its efforts to establish a reliable and effective internal security program throughout the FBI. Aragoncillo, who worked at the FBI from July 2004 until September 2005, was arrested on charges of passing classified documents and information to current and former Philippine government officials. After pleading guilty to four federal charges, including transmission of national defense information, Aragoncillo was sentenced to 10 years in prison in July 2007. In examining the Aragoncillo case, we found that, like Hanssen, Aragoncillo exploited vulnerabilities in the FBI's automated case management system. In addition, the Aragoncillo case highlighted deficiencies in the FBI's efforts to establish an internal security program that effectively detects improper or suspicious employee activity and provides that information to personnel with counterespionage expertise. We concluded that the circumstances surrounding Aragoncillo's activities and the FBI's response to them are stark reminders of the vulnerabilities that persist within the FBI's security program and the need to address these vulnerabilities. We believe that full implementation of our Hanssen report recommendations can help the FBI in this effort.

In response to our follow-up review, the FBI agreed to take steps to fully implement two of the most important recommendations intended to improve its performance in detecting an FBI penetration. The FBI agreed to establish a new unit solely dedicated to determining whether the FBI has been penetrated – a recommendation the FBI previously disagreed with. This unit should improve the FBI's ability to proactively review compromised operations and anomalous personnel security information that suggest an FBI penetration. The FBI also agreed to fill a senior operational position in its Counterespionage Section with a representative from the Central Intelligence Agency or elsewhere in the Intelligence Community. We believe implementing this recommendation can help ensure impartiality and an objective evaluation of source information and other evidence of a possible FBI penetration – factors our original report concluded were lacking when the FBI was searching for the source of what turned out to be Hanssen's espionage.

Sentinel III: Status of the FBI's Development of its Case Management System

The OIG issued its third in a series of audit reports examining the FBI's ongoing development of its Sentinel case management project. The $425 million Sentinel program, which follows the FBI's unsuccessful attempt to develop a modern case management system (Virtual Case File), is intended to move the FBI to an electronic case management system and provide an automated workflow process by December 2009.

Our first audit on Sentinel, released in March 2006, highlighted several concerns about the FBI's progress on Sentinel. Our second audit, issued in December 2006, found that the FBI made progress in addressing most of the concerns highlighted in our first review.

Our current audit focused on the completion of the first of the FBI's planned four-phase implementation of various Sentinel capabilities over a 45-month period. Phase 1 of Sentinel, implemented in June 2007, delivered two key project components: 1) a user-friendly, web-based portal that provides access to information currently in the FBI's antiquated Automated Case Support system; and 2) workboxes that summarize case information and allow supervisors to better manage resources and make assignments. Both

of these Sentinel components should enhance FBI employees' access to information and case management within the FBI.

We found that phase 1 was completed slightly behind schedule and its costs increased a small amount from initial estimates. We also found that one of the four deliverables initially planned for completion in phase 1 was deferred to a later phase for technical reasons. Additionally, because the FBI's expectations for implementing a service-oriented architecture in Phase 1 were vague, we could not assess whether Phase 1 fully achieved its objectives in this area.

Our audit determined that the FBI has made progress addressing most of the concerns we identified in our two previous audits of the Sentinel project. We also found that the FBI has implemented several management controls and processes designed to help it adequately manage the development of Sentinel and bring it to a successful conclusion. However, we concluded that the FBI must make additional progress in the implementation of earned value management, risk management, and the bill of materials.

Our report contained nine new recommendations to the FBI, including to limit the scope and duration of future project phases to make them more manageable, adjust the amount of task orders to reflect changes in project requirements, include both initial and revised performance baselines in earned value management reports, improve the requirements for contract cost reporting, improve risk management and the tracking of project deficiencies, and improve the bill of materials process. The FBI agreed with our recommendations. We will continue to monitor and issue audit reports throughout the Sentinel project.

Follow-up Review of the FBI's Efforts to Hire, Train, and Retain Intelligence Analysts

The OIG's Audit Division completed a follow-up review of the FBI's progress in hiring, training, and retaining intelligence analysts. Since the September 11, 2001, terrorism attacks the FBI has emphasized development of its intelligence analysis capabilities to help meet its highest priority of preventing future attacks. Our 2005 report found that the FBI hired less than 40 percent of the analysts needed to meet its hiring goal, had not determined the total number of analysts needed to support its intelligence mission, and made slow progress toward developing a quality training curriculum for new analysts.

Our follow-up review found that the FBI continued to augment the size of its intelligence analyst workforce by hiring qualified candidates. We found that the FBI increased the number of intelligence analysts by over 50 percent from September 2004 to September 2006. In our prior audit we found that intelligence analysts too often were assigned to perform routine administrative tasks rather than analytical tasks. In this follow-up review, we found that this underutilization of analysts has largely been corrected.

We also found that intelligence analysts continued to express high levels of satisfaction with their work assignments and believed that they were making important contributions to the FBI's mission. The FBI also has begun conducting exit surveys to help further improve the hiring, training, utilization, and retention of its intelligence analysts.

Still, the FBI must make additional improvements to fully implement recommendations in our

previous report. Despite the FBI's hiring of 375 new intelligence analysts in FY 2006, it had a shortfall of 400 analysts from its funded staffing level of 2,574 analysts. In addition, we found that from FYs 2004 to 2006 the average time from when a job announcement closed until an intelligence analyst candidate entered on duty increased from approximately 19 to 31 weeks. Several FBI managers stated that the lengthy screening process may have caused candidates to lose patience and accept employment elsewhere.

Similar to our previous report, a majority of the intelligence analysts we interviewed said the training they received did not meet their expectations for helping them do their job. Additionally, we determined that the professional divide between FBI analysts and special agents remained a concern. Eighty percent of the analysts we interviewed, and all the analysts' supervisors we interviewed, stated that special agents misunderstood the functions and capabilities of intelligence analysts at least some of the time. In our prior report, we recommended that all special agents, not just new agents, receive training on the role and capabilities of intelligence analysts. However, other than a brief exposure through one joint exercise in new analyst and new special agent training, FBI special agents have not received formal training in the function and proper utilization of intelligence analysts.

In total, 10 of the 15 recommendations in our previous report still required additional action and monitoring. We also made new recommendations to evaluate the hiring and background investigation process to identify ways to accelerate the accession of new intelligence analysts, involve intelligence managers and experienced analysts in training curriculum development efforts, and make student and supervisor evaluations of analyst training mandatory. The FBI concurred with our recommendations.

CODIS Audits

The FBI's CODIS includes a national information repository that permits the storing and searching of DNA specimen information to facilitate the exchange of DNA information by law enforcement agencies. During this reporting period, the OIG's Audit Division audited several state and local laboratories that participate in CODIS to determine if they comply with the FBI's Quality Assurance Standards and National DNA Index System (NDIS) requirements. Additionally, we evaluated whether the laboratories' DNA profiles in CODIS databases were complete, accurate, and allowable. Below are examples of our findings:

- Two CODIS-participating laboratories, the Albuquerque Police Department Crime Laboratory Biological Analysis Group (APD) and the New Mexico DNA Identification System Administrative Center (NMDIS), were in compliance with the standards governing CODIS activities with the following exceptions: 1) in 1 out of 10 cases we tested where the CODIS software indicated an interstate candidate match between a known or unknown perpetrator and crime scene evidence, NMDIS did not confirm the match within the time limits specified by the NDIS requirements; 2) due to emergency egress requirements, the APD work area that housed the CODIS server was accessible to non-DNA personnel and thus did not comply with NDIS requirements for the physical security of the CODIS server; 3) APD did not comply with its quality assurance manual because the CODIS manager it designated to address the NDIS requirement for a CODIS administrator was not fully trained; 4) out of 100 forensic profiles tested, we found 1 forensic profile was incomplete because APD did not load all of the required loci into NDIS and 1 forensic

profile was inaccurate because APD did not load the correct specimen number into NDIS; and 5) case files for 16 forensic profiles did not contain clear documentation that all appropriate administrative reviews were performed. Both NMDIS and APD addressed all of our findings.

- The Richland County Sheriff's Department DNA Laboratory in Columbia, South Carolina, was in compliance with the standards governing CODIS activities with the following exceptions: 1) NDIS terminals were not physically secured from unauthorized personnel as required by the memorandum of understanding; and 2) the Laboratory uploaded four forensic profiles into the State DNA Index System that were subsequently uploaded into NDIS, but the profiles were unallowable for NDIS. The Laboratory complied with our recommendations to install the requested magnetic card key reader on the door to the office space where the NDIS terminals reside to adequately secure them, review all profiles uploaded to NDIS to ensure they are allowable, and implement procedures to ensure that CODIS users review uploaded profiles when new case information is obtained from investigators.

Investigations

During this reporting period, the OIG received 903 complaints involving the FBI. The most common allegations made against FBI employees were Intelligence Oversight Board violations, job performance failure, waste, and misuse of government property. The OIG opened 18 cases and referred other allegations to the FBI's Inspection Division for its review.

At the close of the reporting period, the OIG had 35 open criminal or administrative investigations of alleged misconduct related to FBI employees. The criminal investigations covered a wide range of offenses, including release of information, waste, and misuse of government property and personal relationships. The administrative investigations involved serious allegations of misconduct. The following are examples of cases involving the FBI that the OIG's Investigations Division handled during this reporting period:

- An investigation by the OIG's Philadelphia Area Office determined that an FBI special agent deliberately used a false name and social security number to establish an otherwise ineligible person as a confidential informant. Subsequently, the special agent entered into an inappropriate financial relationship with the confidential informant – advancing money to the confidential informant from his personal funds to pay her rent, a 3-year fitness membership, and other items, and then reimbursing himself by withholding part of her informant payments. The investigation also determined that the special agent continued to employ and protect her as a confidential informant despite his personal knowledge that she was engaging in unauthorized criminal activity. The case was declined for prosecution. The special agent retired while under investigation.

- An investigation by the OIG's Miami Field Office determined that an FBI special agent abused prescription narcotics and used his position to obtain prescription medication. The special agent admitted during an interview with OIG investigators that he abused various types of prescription pain medication, informed pharmacists that he was an FBI special agent and showed his credentials and service weapon to prevent questioning

about his prescription drug purchases, and paid cash to avoid detection by his insurance carrier. Criminal prosecution was declined in the Southern District of Florida. The FBI terminated the special agent from his position as a result of the investigation.

- An investigation by the OIG's Philadelphia Area Office determined that an FBI special agent assigned to the Newark Division submitted an official form indicating that a cooperating witness was paid $2,100 in FBI funds when, in fact, bank records and statements from the cooperating witness revealed that he only received $1,500. The USAO for the District of New Jersey declined prosecution of the special agent for theft of government funds relating to the missing $600. The special agent resigned while under investigation.

- An investigation by the OIG's El Paso Area Office determined that an FBI special agent engaged in a sexual relationship with an FBI informant and the sexual relationship likely involved some degree of coercion or intimidation. The USAOs for both the Northern and Southern Districts of Texas declined criminal prosecution of the special agent. The OIG completed its investigation and provided a report to the FBI for appropriate action.

- An investigation by the OIG's Denver Field Office determined that an FBI special agent fraudulently claimed and received reimbursement for $6,832 in lodging expenses that he did not incur. The USAO for the District of Utah declined prosecution. The OIG completed its investigation and provided its report to the FBI for appropriate action.

Ongoing Work

The FBI's Use of National Security Letters and Section 215 Orders

As required by the *USA Patriot Improvement and Reauthorization Act of 2005* (Patriot Reauthorization Act), the OIG is reviewing the FBI's use of national security letters and Section 215 orders for business records in 2006. In the national security letter follow-up review, we also are examining the FBI's corrective actions taken in response to our March 2007 report regarding the use of these authorities in prior calendar years. Part of the report also will discuss the results of the investigation of the FBI's use of exigent letters.

FBI Involvement in and Observations of Detainee Interrogations in Guantanamo Bay, Iraq, and Afghanistan

The OIG is reviewing FBI employees' observations and actions regarding detainee interrogations at Guantanamo Bay, Iraq, and Afghanistan. The OIG is examining whether FBI employees participated in any incident of detainee abuse, whether FBI employees witnessed incidents of abuse, whether FBI employees reported any abuse, and how those reports were handled by the FBI.

The FBI's Efforts to Resolve Terrorist Threats and Suspicious Incidents

FBI guidance requires that terrorist threats and suspicious incidents be reported to the FBI's

National Threat Center Section and be resolved through investigation. Threats and suspicious incidents also are recorded in the FBI's Guardian database, which enables users to enter, assign, and manage the FBI's response to terrorism threats and suspicious activities while simultaneously allowing field offices and Joint Terrorism Task Force members to view this information. Among other issues, the OIG is assessing the process and guidance for recording, resolving, and sharing information on terrorism threats; the FBI's compliance with the proper recording and resolution of threats; and the status of the FBI's IT tools for tracking the resolution of such threats.

The FBI's Efforts to Combat Crimes Against Children

The OIG is auditing the FBI's ability to effectively meet the goals of its Crimes Against Children program. We are assessing the FBI's efforts to establish or enhance initiatives designed to decrease the vulnerability of children to acts of sexual exploitation and abuse; develop a nationwide capacity to provide a rapid, effective, and measured investigative response to crimes involving the victimization of children; and enhance the capabilities of state and local law enforcement investigators through training programs, investigative assistance, and task force operations.

FBI Security Check Procedures for Immigration Applicants

The OIG is examining the FBI's criminal history verification operations and determining how FBI security check procedures impact the accurate and timely completion of immigration applications.

U.S. Marshals Service

The USMS is responsible for protecting more than 2,000 federal judges and other members of the federal judiciary; arresting federal, state, and local fugitives; protecting federal witnesses; transporting federal prisoners; managing assets seized from criminal enterprises; and responding to special assignments. The Director and Deputy Director work with 94 U.S. marshals to direct the work of approximately 4,800 employees at more than 350 locations throughout the 50 states, Guam, Northern Mariana Islands, Puerto Rico, U.S. Virgin Islands, Mexico, Jamaica, and the Dominican Republic.

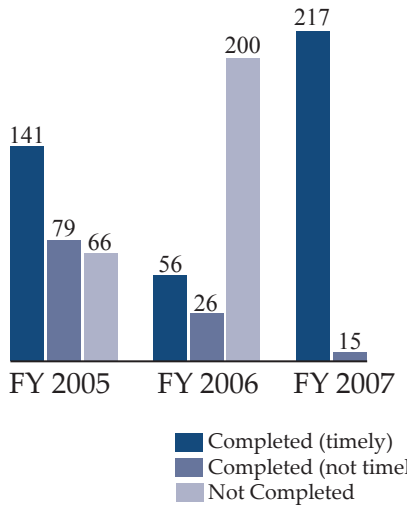
Reports Issued

Follow-up Review of Judicial Security

In September 2007, the OIG's Evaluation and Inspections Division completed a follow-up review of the USMS's progress in evaluating and responding to threats made against federal judges and other court personnel that the USMS protects. The earlier report, issued in March 2004, concluded that the USMS needed to take immediate steps to improve its ability to assess and respond to threats to the federal judiciary. Our September 2007 report found that, while the USMS recently has made some progress, efforts to improve its abilities to assess reported threats and identify potential threats against the judiciary languished until recently.

Our review found that as of October 1, 2006, more than 2 years after issuance of our 2004 report, the USMS had a backlog of 1,190 threat assessments. From our random sample of 568 of the 2,018 threats reported to USMS headquarters in FYs 2005 and 2006, we found that about two-thirds of the threats were not assessed within established timeliness standards. However, beginning in FY 2007 and during our follow-up review, the USMS assigned additional resources to address the backlog and assess new threats more quickly. As a result, the backlog has been eliminated. Yet, the USMS acknowledged that the assessments produced under the current process were of limited utility and further improvements to its threat assessment process were necessary. The USMS stated that it planned to change the threat assessment process in FY 2008.

Assessment of Reported Threats: FY 2005 through FY 2007



Our review also found that the USMS made only limited progress with its Office of Protective Intelligence program, established, in part, to provide a centralized unit to proactively identify potential threats against federal judges, U.S. attorneys, and other court personnel. Three years after its creation, the office lacked the staff to develop protective intelligence on potential threats. Although the USMS added staff to the office beginning in May 2005, the additional resources primarily were assigned to reduce the backlog of pending threats and assess new threats rather than to proactively identify potential threats.

Our review also determined that the USMS successfully implemented a home alarm program for federal judges and as of July 2007 installed about 95 percent of the requested home alarms. An OIG survey of federal judges on safety and security issues resulted in 88 percent responding that they either were "very" or "somewhat" satisfied with the home alarm program. Additionally, 87 percent responded that they either were "very" or "somewhat" satisfied with the USMS's performance in providing protection. In response to questions about measures the USMS should take to further improve judicial security, most judges considered improving intelligence collection and analysis capacity most important.

In addition, we found that the USMS has begun enhancing its Technical Operations Group to provide sophisticated technological support for judicial security investigations and intelligence work. The USMS also said it is developing a Rapid Deployment Team program to respond to significant incidents involving judicial security around the country.

The OIG concluded that the USMS must exhibit a greater sense of urgency in improving its capability to assess reported threats against the judiciary, creating and sharing protective intelligence on potential threats, and completing the implementation of enhanced security measures. We made six recommendations, and the USMS concurred with five.

USMS's Workforce Composition and Utilization

The OIG's Audit Division examined the USMS's workforce management, including its efforts to ensure that an appropriate amount of resources are directed towards the component's highest priorities, such as judicial security and fugitive apprehension.

The USMS faces significant challenges in planning its activities because the bulk of its workload is not self-initiated and instead originates from other agencies and the federal judicial system. Our review found that the USMS has improved its strategic planning and taken positive steps to refine the quantitative models used to determine its resource needs. However, we found several areas in further need of improvement, including weaknesses in the accuracy and comprehensiveness of data in some of the automated systems the USMS uses for resource planning.

The OIG determined that USMS management does not routinely review employee resource utilization reports and could not fully explain inconsistencies between the level of effort recorded and the level of effort officials believed the USMS actually expended on protective investigations, fugitive matters, and the utilization of contract guards. For example, the USMS was unaware that its data systems reflected that the USMS employed just 24 work years on judicial protective investigations in FY 2005, an issue considered a top priority by the component. In contrast, the USMS spent 981 work years on fugitive apprehension matters during the same timeframe. While the USMS

believed that the statistics related to judicial protective investigations were under-reported, this highlights weaknesses in the system the USMS uses to track time spent by its workforce. The OIG determined that periodic employee resource utilization reviews would be beneficial for USMS management to assess whether it was appropriately addressing its highest priority missions.

The OIG also identified weaknesses in the USMS's training program, including a shortage of training opportunities for USMS operational personnel and supervisors beyond their initial academy training. In addition, we found no system that accurately recorded and managed the USMS's training activities and inadequate management of the USMS's training funds.

The OIG made 15 recommendations to assist the USMS in improving its workforce management and planning. The USMS agreed with our recommendations and outlined a plan for corrective action.

Conditions in the Moultrie Courthouse

In response to a request from the Senate Appropriations Committee, the OIG's Evaluation and Inspections Division examined health, safety, and security conditions in areas used by the USMS in the H. Carl Moultrie I Courthouse in Washington, D.C. The Moultrie Courthouse, constructed 31 years ago, houses the District of Columbia Superior Court, Court of Appeals, and Family Court. The USMS provides security for judicial officials and prisoners in the courthouse.

Our review documented 166 serious, uncorrected failures to meet federal health, safety, and security standards in the cellblock and USMS administrative area in the courthouse. These substandard conditions created unacceptable working conditions for the USMS staff assigned to the District of Columbia Superior Court and safety risks for both staff and prisoners.

The OIG found that the District of Columbia Courts have taken some steps to address these issues, but we concluded that the substandard conditions would continue to exist until the Courts and the USMS agreed on health, safety, and security standards that applied to the space and who would be responsible for requesting funds to repair and improve the space to meet these standards.

Investigations

During this reporting period, the OIG received 216 complaints involving the USMS. The most common allegations made against USMS employees included official misconduct and force, abuse, and rights violations. The OIG opened 14 investigations and referred other allegations to the USMS's Office of Internal Affairs for review.

At the close of the reporting period, the OIG had 20 open cases of alleged misconduct against USMS employees. The following is an example of a case involving the USMS that the OIG's Investigations Division handled during this reporting period:

- An investigation by the OIG's Dallas Field Office led to the arrest and guilty plea of a deputy U.S. marshal (DUSM) in the Southern District of Texas on charges of exceeding authorized computer access for financial gain. The investigation determined that the DUSM, a 17-year USMS employee, accepted multiple bribes totaling approximately $6,000 from a confidential informant in exchange for providing sensitive law enforcement information to the informant on numerous occasions. The DUSM resigned from his position as a result of our investigation. Sentencing is pending.

Federal Bureau of Prisons

The BOP operates a nationwide system of prisons and detention facilities to incarcerate those imprisoned for federal crimes and detain those awaiting trial or sentencing in federal court. The BOP has approximately 36,000 employees and operates 114 institutions, 6 regional offices, and 2 staff training centers. The BOP is responsible for the custody and care of approximately 199,000 federal offenders, 166,600 of whom are confined in BOP-operated correctional institutions and detention centers. The remainder are confined in facilities operated by state or local governments or in privately operated facilities.

Investigations

During this reporting period, the OIG received 3,144 complaints involving the BOP. The most common allegations made against BOP employees included official misconduct and force, abuse, and rights violations. The vast majority of complaints dealt with non-criminal issues that the OIG referred to the BOP's Office of Internal Affairs for review.

At the close of the reporting period, the OIG had 251 open cases of alleged misconduct against BOP employees. The criminal investigations covered a wide range of allegations, including introduction of contraband, bribery, and sexual abuse. The following are examples of cases involving the BOP that the OIG's Investigations Division handled during this reporting period:

- An investigation by the OIG's New York Field Office led to the arrest of 11 BOP correctional officers charged with violating the civil rights of 2 inmates at the Metropolitan Detention Center in Brooklyn, New York. According to the indictment, in November 2002 five correctional officers participated in a planned beating of an inmate and then attempted to disguise the attack by claiming in written reports that the inmate became combative as they attempted to prevent him from committing suicide. According to the indictment, in a second incident in April 2006 five correctional officers, including one who participated in the previously described attack, physically assaulted an inmate in an elevator while escorting him to a special housing unit within the facility. These five correctional officers and two additional officers were charged with writing false reports concerning this incident. The case is being prosecuted by the USAO for the Eastern District of New York. Several of the defendants pled guilty to these offenses, and trials on the remaining defendants are upcoming.

- A joint investigation by the OIG's Chicago Field Office and the FBI led to the conviction of a correctional officer who conspired with relatives of inmates at the U.S. Penitentiary in Big Sandy, Kentucky, to introduce drugs into the facility. The investigation determined

that the correctional officer met with inmates' relatives at a local motel and accepted bribes to bring contraband into the prison. The correctional officer was convicted at trial and sentenced in the Eastern District of Kentucky to 78 months' incarceration followed by 36 months' supervised release. One civilian involved in the case also was convicted at trial and sentenced to 21 months' incarceration followed by 36 months' supervised release. In addition, two inmates and two other civilians pled guilty and were sentenced. The correctional officer also was terminated from her position.

- An investigation by the OIG's Los Angeles Field Office led to two BOP correctional officers assigned to the Federal Correctional Complex in Lompoc, California, being sentenced on charges of bribery and introduction of contraband. The OIG investigation determined that one of the correctional officers accepted $10,000 in bribes in exchange for smuggling contraband, including tennis shoes, gloves, nutritional supplements, sunglasses, and iPods, into the institution. The second correctional officer met with an undercover agent and accepted 5 ounces of black tar heroin, an iPod, and a $7,500 bribe in exchange for smuggling contraband into the institution. The first correctional officer was sentenced to 18 months' incarceration followed by 24 months' supervised release. The second correctional officer was sentenced to 30 months' incarceration followed by 24 months' supervised release. Both correctional officers resigned from the BOP as a result of our investigation.

- An investigation by the OIG's Washington Field Office led to the arrest and guilty plea of a BOP Federal Prison Industries, Inc. (UNICOR) general manager, previously assigned to the UNICOR Central Office in Washington, D.C., to a conflict of interest violation. Investigators developed evidence that in early 2004 the UNICOR general manager negotiated a post-government position with a UNICOR vendor with whom he was substantially involved in his capacity as general manager. After accepting an offer of future employment, the UNICOR general manager directed a $250,000 sole source contract to the vendor without disclosing his financial interest in the matter to anyone in the government. The UNICOR general manager retired 3 months later and began working for the vendor, collecting $20,000 in salary over the next 5 months. Sentencing in the Western District of Tennessee is pending.

- An investigation by the OIG's Houston Area Office led to the arrest of a BOP special investigative supervisor technician assigned to the Federal Correctional Institution in Beaumont, Texas, on charges of bribery, smuggling contraband into a federal prison, sexual abuse of a ward, and possession with intent to distribute a controlled substance. The investigation disclosed that the special investigative supervisor technician engaged in a sexual relationship with an inmate; accepted a $950 monetary bribe for smuggling personal hygiene products, weight lifting supplements, and a cellular telephone into the prison; and stole marijuana from the special investigative supervisor evidence locker and provided it to an inmate. Judicial proceedings continue.

- An investigation by the OIG's Miami Field Office led to the arrest of four BOP correctional officers assigned to the Rivers Correctional Institution, a BOP contract facility located in Winton, North Carolina. The investigation determined that the four correctional officers assaulted an inmate during a dispute regarding a food tray and submitted

memoranda to the BOP that contained false information relating to the incident. Sentencing is pending for two of the correctional officers who pled guilty and resigned from their positions. Judicial proceedings continue for the other two correctional officers.

- A joint investigation by the OIG's Tucson Area Office, FBI, and BOP led to the arrest and guilty plea of a BOP electronics technician assigned to the Federal Correctional Institution in Phoenix, Arizona, on a charge of making false statements. The investigation determined that the electronic technician had sexual contact with and provided prohibited items to female inmates who were detained at the Phoenix Federal Prisons Camp. During this investigation, the technician denied both his relationship with the inmates and providing the inmates with soft contraband. The technician resigned from his position as a result of our investigation. Sentencing is pending.

Ongoing Work

The BOP's Efforts to Manage Inmate Health Care

The BOP is required to provide medical, dental, and mental health care to inmates in its custody. However, escalating health care costs have challenged the BOP's ability to meet the health care needs of an aging inmate population in a cost-effective manner. The OIG is auditing whether the BOP is providing necessary health care services and effectively administering its medical services contracts and monitoring its medical services providers.

The BOP's Administration of the Witness Security Program

The Witness Security Program provides protection to federal witnesses and their family members. The OIG previously audited the USMS's and the Criminal Division's role in the Witness Security Program. Our third audit in this series is assessing the BOP's role in the Program, including the BOP's security for Witness Security Program prisoners in its custody.

Review of Health and Safety Issues at BOP Computer Recycling Facilities

The OIG is investigating whether the BOP adequately addressed allegations that workers and inmates at several BOP institutions were exposed to unsafe levels of lead, cadmium, and other hazardous materials in computer recycling plants operated by UNICOR.

Bureau of Alcohol, Tobacco, Firearms and Explosives

ATF's 5,000 employees perform the dual responsibilities of enforcing federal criminal laws and regulating the firearms and explosives industries. ATF investigates violent crime involving firearms and explosives, acts of arson, and illegal trafficking of alcohol and tobacco products. ATF also provides training and support to its federal, state, local, and international law enforcement partners and works in 23 field divisions with representation throughout the United States, Puerto Rico, U.S. Virgin Islands, and Guam. Foreign offices are located in Mexico, Canada, Colombia, and representatives in France.

Reports Issued

Investigative Operations at Gun Shows

The OIG's Evaluation and Inspections Division reviewed the policies, procedures, and oversight mechanisms that guide ATF's investigative operations at gun shows across the nation. These operations received widespread attention in February 2006 when Congress held two hearings on ATF law enforcement techniques.

The OIG found that ATF does not have a formal gun show enforcement program, but instead conducts investigative operations at gun shows when it has law enforcement intelligence that illegal firearms activity has occurred or is likely to occur at specific gun shows. We found that ATF conducted operations at 195 gun shows, or 3.3 percent of the estimated 6,000 gun shows held during our 2-year study period of FYs 2004 to 2006. Those operations resulted in 121 arrests and 83 convictions of individuals engaged in firearms trafficking and seizures of 5,345 firearms that were purchased or offered for sale illegally. The OIG found that ATF conducted 77 percent of its investigative operations at gun shows as part of ongoing investigations of specific suspects whose illegal activity happened to occur at gun shows. The remaining 23 percent of these ATF investigative operations were conducted in response to intelligence that widespread illegal firearms activity was occurring specifically at gun shows in particular cities, states, or geographic regions.

The OIG also reviewed operational plans for investigative operations at gun shows and found that these plans generally complied with ATF Headquarters' policies and procedures. In addition, five of seven gun show promoters and all state and local law enforcement personnel interviewed by the OIG were supportive of ATF operations

at gun shows. Only the two Richmond-area gun show promoters, whose shows were involved in the congressional hearings, expressed concern about ATF's activities at gun shows. The OIG review found that, with the exception of the Richmond-area gun shows, ATF conducted its investigative operations at gun shows covertly without incident and without complaints from promoters, vendors, or the public.

National Firearms Registration and Transfer Record

At the request of Congress, the OIG's Evaluation and Inspections Division reviewed ATF's effectiveness in maintaining the records of registrations and transfers of weapons covered by the *National Firearms Act* (NFA). Congress passed the NFA in 1934 to limit the availability of machine guns, short-barreled shotguns, short-barreled rifles, silencers, and other similar weapons that often were used by criminals. NFA imposed a tax on the manufacture, import, and distribution of the weapons it covered and required ATF to collect the taxes and maintain NFA weapon ownership records in a central registry, called the National Firearms Registration and Transfer Record (NFRTR), which is maintained by ATF's NFA Branch.

Our evaluation found that since 2004 the NFA Branch has significantly improved its processing time for applications to register or transfer ownership of NFA weapons and its process for responding to customer inquiries. However, we also found that management and technical deficiencies have limited ATF's ability to adequately address errors in the NFRTR database. The NFA Branch staff has not processed applications or entered database information uniformly, which has resulted in errors in records, reports, and queries as well as inconsistent decisions on NFA weapons registration and transfer applications. The processes were not uniform because: 1) the NFA Branch has not established adequate standard operating procedures for processing applications and working with the NFRTR, 2) NFA Branch staff members did not receive any structured training when they were hired, 3) NFA Branch managers did not communicate regularly with staff members, and 4) staff members who reviewed and processed applications received conflicting direction from their supervisors.

Further, the NFA Branch was not timely in correcting errors and discrepancies in the NFRTR database after problems were identified by ATF investigators during compliance inspections of federal firearms licensees. However, we did not find evidence that individual weapons owners or federal firearms licensees were sanctioned or criminally prosecuted because of errors in the database.

The OIG made eight recommendations to help improve the processing of NFA applications and reduce errors in the NFRTR, including that ATF develop comprehensive, standard operating procedures for the NFA Branch and standard training for its staff, as well as an action plan to fix the technical programming flaws and errors in the NFRTR database. ATF concurred with our recommendations.

Investigations

The following is an example of a case involving ATF that the OIG's Investigations Division handled during this reporting period:

- An investigation by the OIG's Miami Field Office developed evidence that an ATF

special agent conducted unauthorized National Crime Information Center checks and disclosed sensitive law enforcement information to her husband in order to assist him in his job. Additionally, the investigation determined that the special agent offered to obtain information for her husband related to investigations of her husband's employer. The USAO for the Southern District of Alabama declined prosecution. The OIG completed its investigation and provided its report to ATF for appropriate action.

Ongoing Work

ATF's Controls over Weapons, Laptops, and Other Sensitive Property

The OIG is examining the effectiveness of ATF's controls over weapons, ammunition, explosives, and laptop computers, as well as the adequacy of its actions taken in response to weapons, ammunition, explosives, and laptop computers identified as lost or stolen.

Drug Enforcement Administration

The DEA enforces federal laws and regulations related to the growth, production, or distribution of controlled substances. In addition, the DEA seeks to reduce the supply of and demand for illicit drugs, both domestically and internationally. The DEA has approximately 10,900 employees staffing its 23 division offices in the United States and the Caribbean and 86 offices in 62 other countries.

Investigations

During this reporting period, the OIG received 203 complaints involving the DEA. The most common allegations made against DEA employees included job performance failure, off-duty misconduct, waste, and mismanagement. The OIG opened 8 investigations and referred other allegations to the DEA's Office of Professional Responsibility for review.

At the close of the reporting period, the OIG had 15 open cases of alleged misconduct against DEA employees. The most common allegations were release of information and theft. The following are examples of cases involving the DEA that the OIG's Investigations Division handled during this reporting period:

- An investigation by the OIG's Dallas Field Office led to the arrest and guilty plea of a DEA special agent in the Southern District of Texas on charges of making false statements. The OIG investigation revealed that the special agent conducted multiple queries for a confidential informant using law enforcement databases while also requesting and accepting "loans" from the informant. When approached by the OIG, the special agent denied providing information to or accepting money from the informant. During a second interview, however, the special agent acknowledged providing information to the informant and providing false statements to the OIG. Sentencing is pending.

- In our March 2007 *Semiannual Report to Congress*, we reported on an investigation by the OIG's Denver Field Office that determined a DEA special agent fraudulently obtained a government-funded permanent change of duty station transfer by falsely claiming that his wife suffered from cancer. The DEA expended $47,805 to relocate the special agent and his family. During this reporting period, the special agent and his wife entered into a civil settlement in the District of Utah federal court based on a civil complaint filed under the provisions of the *False Claims Act*. The special agent agreed to reimburse the government $60,000 over a period of 5 years. The special agent resigned from his position as a result of our investigation.

- In our March 2007 *Semiannual Report to Congress*, we reported on a joint investigation

by the OIG's Los Angeles Field Office and the DEA's Office of Professional Responsibility that resulted in the arrest of a DEA contracting officer on charges of corruptly profiting from his employment as a federal agent and making a false statement. The joint investigation developed evidence that the contracting officer received for his personal use 21 checks totaling $13,442 from a DEA vendor whose contract he managed. The contracting officer also failed to disclose on his financial disclosure form the funds he received from the vendor. During this reporting period, the contracting officer was sentenced on conflict of interest charges. He was sentenced to 2 years' probation and ordered to pay a $13,517 fine and perform 50 hours community service.

Ongoing Work

Follow-up Review of the DEA's Controls over Weapons and Laptop Computers

In August 2002, the OIG issued a report on the DEA's internal controls over its weapons and laptop computers that detailed significant lapses in the control over management of these assets. This follow-up review is examining the inventory of weapons and laptop computers at DEA headquarters and field locations, assessing actions taken by the DEA regarding lost or stolen weapons and laptop computers, and evaluating the DEA's control over its weapons and laptop computers.

The DEA's Utilization of Intelligence Analysts and Reports Officers

The OIG is examining the DEA's efforts to recruit, train, and retain its intelligence analysts and reports officers.

Diversion Control Fee Account

The OIG is reviewing the DEA's use of funds from its diversion control fee account.

Office of Justice Programs

OJP manages the majority of the Department's grant programs and is responsible for developing initiatives to address crime at the state and local level. OJP has approximately 600 employees and is composed of 5 bureaus – Bureau of Justice Assistance (BJA), Bureau of Justice Statistics, National Institute of Justice (NIJ), Office of Juvenile Justice and Delinquency Prevention (OJJDP), and Office for Victims of Crime (OVC) – as well as the Community Capacity Development Office.

Reports Issued

Audits of OJP Grants to State and Local Entities

During this reporting period, the OIG continued to conduct audits of grants awarded by OJP. Examples of findings from these audits included the following:

- Boat People S.O.S. (BPSOS) is a non-profit organization based in Falls Church, Virginia, that provides legal and social services for human trafficking victims. In January 2003, OJP awarded a 3-year, $1.89 million grant to BPSOS and its sub-grantee, Ayuda Inc. of Washington, D.C., to develop, expand, and strengthen victim services during the pre-certification period for persons who have been identified as victims of severe forms of human trafficking. The grantee also received a 1-year, no-cost extension until December 31, 2006. Our audit found that BPSOS and Ayuda spent $700,000 in grant funds either for unsupported or unallowable costs, including providing inadequate supporting documentation for local match transactions, which resulted in unsupported *pro bono* attorney fees of $294,575. Additionally, BPSOS did not accomplish many of its grant objectives. Our report contained 22 recommendations, of which OJP agreed with 21.

- NIJ awarded three Forensic Casework DNA Backlog Reduction Program cooperative agreements totaling more than $7.47 million to the Texas Department of Public Safety (TDPS) in Austin, Texas. We found that the TDPS complied with grant requirements in six of the eight areas we tested. However, we found weaknesses in the areas of budget management and control and cooperative agreement expenditures. For example, TDPS authorized a major budget change of $920,700 with insufficient approval from NIJ. Further, we found unsupported expenditures resulting in questioned costs totaling $3,673. OJP agreed with our recommendations and indicated that additional coordination was required to remedy the $924,373 in total questioned costs.

Investigations

The following are examples of cases involving OJP that the OIG's Investigations Division handled during this reporting period:

- A joint investigation by the OIG's Fraud Detection Office and the FBI resulted in the arrest of the Lawton Outreach Center Director on a charge of bank fraud. OIG investigators found that the Director falsely represented that the Board of Directors of the Lawton Outreach Center, which is an OJP grantee located in Lawton, Oklahoma, authorized her to apply for a bank loan of $22,913. The Director used office equipment purchased with OJP grant funds as collateral for the loan. When issues of the Director's mismanagement of funds surfaced, the Lawton Weed and Seed Steering Committee, which oversees the Center, dismissed the Director and ended its relationship with the Lawton Outreach Center. Judicial proceedings continue.

- An investigation by the OIG's Fraud Detection Office led to the arrest and indictment in the Western District of Oklahoma of three OJP grantees on charges of conspiracy, theft, and aiding and abetting. In September 2002, the Office on Violence Against Women (OVW) awarded a $299,815 grant to the South Central Region Tribal Nations and Friends Domestic Violence Coalition to assist in its efforts to support victims of domestic violence. However, our investigation determined that the executive director of the Coalition stole over $100,000 in grant funds, and two board members of the Coalition stole approximately $25,000 and $37,000, respectively. Judicial proceedings continue.

Ongoing Work

Southwest Border Prosecution Initiative

Administered by OJP, the Southwest Border Prosecution Initiative (SWBPI) reimburses eligible jurisdictions in the four southwest border states for costs associated with the prosecution of criminal cases declined or referred by local USAOs. The OIG is auditing the effectiveness of OJP's administration and oversight of SWBPI reimbursements, and whether SWBPI reimbursements are allowable and supported in accordance with applicable laws, rules, and regulations.

Management of the Grant Program for Human Trafficking Victims

OVC provides grants to support victim service programs for alien victims trafficked into or within the United States who require emergency services. The OIG is examining the extent to which the grant program has achieved its objective to provide effective assistance for victims of trafficking.

Hometown Heroes Survivors Benefits

The OIG is reviewing OJP's implementation of the *Hometown Heroes Survivors Benefits Act of 2003*, which allows payment of public safety officer survivor benefits for fatal heart attacks or strokes suffered in the line of duty. The review is determining whether OJP is processing death claims for heart attacks and strokes in a timely manner and in accordance with the intent of the Act.

Other Department Components

U.S. Attorneys' Offices

U.S. attorneys serve as the federal government's principal criminal and civil litigators and conduct most of the trial work in which the United States is a party. Under the direction of the Attorney General, 93 U.S. attorneys are stationed throughout the United States, Puerto Rico, U.S. Virgin Islands, Guam, and Northern Mariana Islands. More than 10,800 employees work in those offices and in the Executive Office for U.S. Attorneys.

Investigations

The following are examples of cases involving the USAOs that the OIG's Investigations Division handled during this reporting period:

- An investigation by the OIG's Miami Field Office resulted in the arrest and guilty plea of a Law Enforcement Coordinating Committee liaison assigned to the USAO in the Southern District of Alabama on charges of theft of public property. The investigation developed evidence that the liaison, in his collateral duty as the public information officer, obtained sensitive information on a federal grand jury investigation and provided that information to unauthorized persons. During his initial interview with the OIG, the public information officer denied providing sensitive information to unauthorized persons. However, during a subsequent interview and polygraph examination he admitted to disclosing information pertaining to a federal grand jury investigation to unauthorized persons. The public information officer resigned from his position with the USAO as a result of the investigation. Sentencing is pending.

- An investigation by the OIG's Chicago Field Office resulted in the arrest and guilty plea of a legal assistant employed at the USAO in the Eastern District of Wisconsin on charges of mail fraud. OIG investigators developed evidence that, while employed at the USAO, the legal assistant applied for and received unemployment benefits from the State of Wisconsin totaling $8,698. The State of Wisconsin was reimbursed for the unemployment benefits by drawing down funds from a U.S. Treasury account maintained for that purpose. The USAO terminated the legal assistant from her position as a result of our investigation. Sentencing is pending.

Ongoing Work

Review of Resource Management in the U.S. Attorneys Offices

The OIG is auditing the allocation of resources of the 93 U.S. attorneys. In particular, the audit is determining the criminal and civil areas to which federal prosecutors are allocated and utilized, as well as the type and number of cases being handled by USAOs.

Criminal Division

Reports Issued

Equitable Sharing Audits

Under the Department's Forfeiture Program, state and local law enforcement agencies receive equitable sharing assets when participating directly with the Department's law enforcement components in joint investigations that lead to the seizure or forfeiture of cash and property. To be eligible to receive equitable sharing proceeds, law enforcement agencies must submit a sharing request within 60 days of an asset seizure.

During this reporting period, the OIG's Audit Division audited the Colorado State Patrol (CSP), a division of the Colorado Department of Public Safety, and the Boulder County, Colorado, Drug Task Force (BCDTF) and reviewed each auditee's compliance with six essential equitable sharing guidelines.

The Department awarded CSP with equitable sharing revenues totaling more than $1 million and property valued at $10,737 to support law enforcement operations. We identified six non-compliance issues, including $135,570 in questioned costs related to expenditures of equitable sharing revenues for unallowable purposes. We made seven recommendations, including requiring the CSP to remedy the questioned costs, accurately account for equitable sharing revenue expenditures, discontinue the practice of moving lump sum costs into and out of the equitable sharing revenue fund, and use forfeited tangible property for law enforcement purposes only. The Criminal Division and CSP agreed with six of the recommendations.

The Department awarded BCDTF with equitable sharing revenues totaling more than $1.1 million and property valued at $15,611 to support law enforcement operations. We found that the BCDTF generally complied with the guidelines. However, we found weaknesses in the following areas: 1) the Annual Certification Reports submitted for FYs 2005 and 2006 contained inaccurate information, 2) a new Federal Sharing Agreement was not submitted when an administration change occurred, and 3) $88,352 in questioned costs were identified related to transfers of equitable sharing revenues from the BCDTF to participating agencies that did not submit the required Federal Equitable Sharing Agreement. We made three recommendations, and the Criminal Division and BCDTF agreed with the recommendations.

Office of Community Oriented Policing Services

Reports Issued

COPS Grant Audits

During this reporting period, the OIG audited various grants awarded by COPS. The purpose of our audits are to determine whether the costs reimbursed under the grants were allowable; supported; and in accordance with applicable laws, regulations, guidelines, and the terms and conditions of the grant. The following is an example of findings from OIG audits issued during this reporting period:

The OIG audited COPS' $4 million grant to the City of Philadelphia Police Department (PPD) to fund police overtime for its Operation Safe Streets program and Counter-Terrorism Bureau. The PPD received a $3 million grant in September 2003 and contributed an additional $1 million for a required 25-percent share of its total program costs. We determined that the PPD did not fully comply with the grant requirements we tested. We reviewed compliance with six essential grant conditions and found material weaknesses in the areas of grant expenditures, matching expenditures, reporting, and program performance. COPS agreed with our 15 recommendations, including the questioned costs of $1.2 million.

Environment and Natural Resources Division

Reports Issued

Superfund Audit for Fiscal Years 2004 and 2005

The *Comprehensive Environmental Response, Compensation, and Liability Act of 1980* (Superfund) provides for liability, compensation, cleanup, and emergency response for hazardous substances released into the environment and for uncontrolled and abandoned hazardous waste sites. The Department conducts and controls all litigation arising under Superfund and is reimbursed through interagency agreements with the Environmental Protection Agency (EPA). These agreements authorize reimbursement to the Department's Environment and Natural Resources Division (ENRD) for direct and indirect litigation costs. ENRD contracted with an accounting firm to maintain a system of

accounting controls to document Superfund litigation costs. The EPA authorized ENRD reimbursements of $27.9 million for FY 2004 and $26.9 million for FY 2005 in accordance with the Interagency Agreements.

As required by Superfund, the OIG audited the cost allocation process used by ENRD and its contractor to see if it provided an equitable distribution of total labor costs, other direct costs, and indirect costs to Superfund cases during FYs 2004 and 2005. We compared costs reported on the contractor-developed accounting schedules and summaries for FYs 2004 and 2005 to the information recorded on the Department's accounting records, and we reviewed the cost distribution system used by ENRD to allocate incurred costs to Superfund and non-Superfund cases. Based on the results of the audit, we concluded that ENRD provided an equitable distribution of total labor costs, other direct costs, and indirect costs to Superfund cases during FYs 2004 and 2005. However, we recommended that ENRD update its case designation procedures, ensure that travel authorizations are approved prior to the traveler proceeding on the trip, and ensure that all subject code 2508 transactions are allocated to the correct Superfund case number.

Tax Division

Investigations

The following is an example of a case involving the Tax Division that the OIG's Investigations Division handled during this reporting period:

- A joint investigation by the OIG's Washington Field Office and the FBI led to the arrest of a paralegal specialist pursuant to an indictment returned in the Eastern District of Virginia on charges of harboring and concealing an FBI fugitive from arrest. The investigation determined that the paralegal specialist in the Tax Division knowingly harbored and concealed an FBI fugitive for over a year by allowing him to reside with her in Virginia and also by purchasing a residence for him in West Virginia. The Tax Division placed the paralegal specialist on leave without pay while her sentencing is pending.

Executive Office for U.S. Trustees

Ongoing Work

Monitoring and Oversight of Chapter 7 Panel Trustees

The OIG is auditing the U.S. Trustee Program's monitoring and oversight of Panel Trustees who collect, liquidate, and distribute personal and business cases under Chapter 7 of the Bankruptcy Code.

Top Management and Performance Challenges

The OIG has created a list of top management and performance challenges in the Department annually since 1998, initially in response to congressional requests but in recent years as part of the Department's annual *Performance and Accountability Report*.

The top challenges for this year are listed below. The challenges are not presented in order of priority – we believe that all are critical management and performance issues facing the Department. However, it is clear that the top challenge facing the Department is its ongoing response to the threat of terrorism. Several other top challenges are closely related to and impact directly on the Department's counterterrorism efforts.

This year, we added the challenge of "Restoring Confidence in the Department of Justice." The Department has faced significant criticism of its actions that has affected the morale of Department employees and the public confidence in the decisions of Department leaders. This turmoil, combined with numerous high-level vacancies, creates a significant challenge for Department leaders to reestablish public confidence in the independence and integrity of the Department.

Top Management and Performance Challenges in the Department of Justice – 2007

1. Counterterrorism
2. Sharing of Intelligence and Law Enforcement Information
3. Information Technology Planning, Implementation, and Security
4. Financial Management and Systems
5. Grant Management
6. Detention and Incarceration
7. Violent Crime
8. Civil Rights and Civil Liberties
9. Cybercrime
10. Restoring Confidence in the Department of Justice

Detailed information about these management and performance challenges can be found online at http://www.usdoj.gov/oig/challenges/index.htm.

Congressional Testimony

On July 11, 2007, the Inspector General testified before the Senate Committee on Homeland Security and Governmental Affairs at a hearing concerning how to strengthen the unique role of Inspectors General.

Legislation and Regulations

The IG Act directs the OIG to review proposed legislation and regulations relating to the programs and operations of the Department. Although the Department's Office of Legislative Affairs reviews all proposed or enacted legislation that could affect the Department's activities, the OIG independently reviews proposed legislation that affects it and legislation that relates to waste, fraud, or abuse in the Department's programs or operations.

During this reporting period, the OIG commented on proposed amendments to the *Inspector General Act*, which is designed to strengthen the independence and accountability of Inspectors General.

Statistical Information

Audit Statistics

Audit Summary

During this reporting period, the OIG's Audit Division issued 137 audit reports containing more than $22 million in questioned costs and more than $350,000 in funds recommended to be put to better use and made 330 recommendations for management improvement. Specifically, the Audit Division issued 16 internal audit reports of Department programs funded at more than $6 billion; 51 external audit reports of contracts, grants, and other agreements funded at more than $148 million; and 70 *Single Audit Act* audits. In addition, the Audit Division issued 17 Notifications of Irregularities, 2 Investigative Assistance Memoranda, 2 Management Improvement Memoranda, and 1 Technical Assistance Memorandum.

Funds Recommended to Be Put to Better Use

Audit Reports	Number of Audit Reports	Funds Recommended to Be Put to Better Use
No management decision made by beginning of period	6	$64,337,546
Issued during period	4	$351,449
Needing management decision during period	10	$64,688,995
Management decisions made during period:		
◆ Amounts management agreed to put to better use[1]	7	$61,637,611
◆ Amounts management disagreed to put to better use	0	$0
No management decision at end of period	3	$3,051,384

[1] *Includes instances in which management has taken action to resolve the issue and/or the matter is being closed because remedial action was taken.*

Audits with Questioned Costs

Audit Reports	Number of Audit Reports	Total Questioned Costs (including unsupported costs)	Unsupported Costs
No management decision made by beginning of period	20	$301,372,475	$4,723,576
Issued during period	36	$22,134,825	$11,992,066
Needing management decision during period	56	$323,507,300	$16,715,642
Management decisions made during period:			
◆ Amount of disallowed costs[1]	50[2]	$314,616,606	$13,550,368
◆ Amount of costs not disallowed	0	$0	$0
No management decision at end of period	7	$8,890,694	$3,165,274

[1] Includes instances in which management has taken action to resolve the issue and/or the matter is being closed because remedial action was taken.

[2] One audit report was not resolved during this reporting period because management has agreed with some but not all of the questioned costs in the audit.

Audits Involving Recommendations for Management Improvements

Audit Reports	Number of Audit Reports	Total Number of Management Improvements Recommended
No management decision made by beginning of period	40	147
Issued during period	94	330
Needing management decision during period	134	477
Management decisions made during period:		
◆ Number management agreed to implement[1]	123[2]	439
◆ Number management disagreed with	1	4
No management decision at end of period	14	34

[1] Includes instances in which management has taken action to resolve the issue and/or the matter is being closed because remedial action was taken.

[2] Includes four audit reports that were not resolved during this reporting period because management has agreed to implement a number of but not all recommended management improvements in these audits.

Audit Follow-up

OMB Circular A-50

OMB Circular A-50, *Audit Follow-up*, requires audit reports to be resolved within 6 months of the audit report issuance date. Audit monitors the status of open audit reports to track the audit resolution and closure process. As of September 30, 2007, the OIG has closed 119 audit reports and was monitoring the resolution process of 356 open audit reports.

Unresolved Audits

Audits Over 6 Months Old without Management Decisions

As of September 30, 2007, the following audits had no management decision or were in disagreement:

- COPS Grants to the Passamaquoddy Tribe and Pleasant Point Reservation Police Department, Perry, Maine
- Oversight of Intergovernmental Agreements by the USMS and the Office of the Federal Detention Trustee
- The DEA's International Operations
- USMS Intergovernmental Service Agreement for Detention Facilities with the Blount County, Tennessee, Sheriff's Office
- USMS Intergovernmental Service Agreement for Detention Facilities with the Central Virginia Regional Jail
- USMS Intergovernmental Service Agreement for Detention Facilities with the Cumberland County Jail, Portland, Maine
- USMS Intergovernmental Service Agreement for Detention Facilities with the Doña Ana County Detention Center, Las Cruces, New Mexico
- USMS Intergovernmental Service Agreement for Detention Facilities with the Hamilton County, Tennessee, Silverdale Correctional Facility
- USMS Intergovernmental Service Agreement for Detention Facilities with the Western Tidewater Regional Jail, Suffolk, Virginia

Evaluation and Inspections Statistics

The chart below summarizes the Evaluation and Inspections Division's (E&I) accomplishments for the 6-month reporting period ending September 30, 2007.

E&I Workload Accomplishments	Number of Reviews
Reviews active at beginning of period	8
Reviews initiated	4
Final reports issued	6
Reviews active at end of reporting period	6

Unresolved Reviews

DOJ Order 2900.10, *Follow-up and Resolution Policy for Inspection Recommendations by the OIG*, requires reports to be resolved within 6 months of the report issuance date. As of September 30, 2007, no unresolved recommendations met this criterion.

Investigations Statistics

The following chart summarizes the workload and accomplishments of the Investigations Division during the 6-month period ending September 30, 2007.

Source of Allegations	
Hotline (telephone and mail)	1,089
Other sources	4,061
Total allegations received	5,150
Investigative Caseload	
Investigations opened this period	220
Investigations closed this period	197
Investigations in progress as of 9/30/07	395
Prosecutive Actions	
Criminal indictments/informations	76
Arrests	69
Convictions/Pleas	39
Administrative Actions	
Terminations	24
Resignations	87
Disciplinary action	31
Monetary Results	
Fines/Restitutions/Recoveries	$239,927
Seizures	$500
Bribe monies deposited to the Treasury	$13,000
Civil penalties	$12,000

Integrity Awareness Briefings

OIG investigators conducted 109 Integrity Awareness Briefings for Department employees throughout the country. These briefings are designed to educate employees about the misuse of a public official's position for personal gain and to deter employees from committing such offenses. The briefings reached more than 2,653 employees.

Appendix 1

Acronyms and Abbreviations

The following are acronyms and abbreviations widely used in this report.

ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
BOP	Federal Bureau of Prisons
BJA	Bureau of Justice Assistance
CODIS	Combined DNA Index System
COPS	Office of Community Oriented Policing Services
DEA	Drug Enforcement Administration
Department	U.S. Department of Justice
FBI	Federal Bureau of Investigation
FISMA	*Federal Information Security Management Act*
FY	Fiscal year
IG Act	*Inspector General Act of 1978*
IT	Information technology
JMD	Justice Management Division
OIG	Office of the Inspector General
OJJDP	Office of Juvenile Justice and Delinquency Prevention
OJP	Office of Justice Programs
OVC	Office for Victims of Crime
OVW	Office on Violence Against Women
OMB	Office of Management and Budget
NIJ	National Institute of Justice
NSA	National Security Agency
TSC	Terrorist Screening Center
Patriot Reauthorization Act	*USA Patriot Improvement and Reauthorization Act of 2005*
USAO	U.S. Attorneys' Offices
USMS	U.S. Marshals Service

Appendix 2

Glossary of Terms

The following are definitions of specific terms as they are used in this report.

Alien: Any person who is not a citizen or national of the United States.

Combined DNA Index System: A distributed database with three hierarchical levels that enables federal, state, and local forensic laboratories to compare DNA profiles electronically.

External Audit Report: The results of audits and related reviews of expenditures made under Department contracts, grants, and other agreements. External audits are conducted in accordance with the Comptroller General's Government Auditing Standards and related professional auditing standards.

Information: Formal accusation of a crime made by a prosecuting attorney as distinguished from an indictment handed down by a grand jury.

Internal Audit Report: The results of audits and related reviews of Department organizations, programs, functions, computer security and IT, and financial statements. Internal audits are conducted in accordance with the Comptroller General's Government Auditing Standards and related professional auditing standards.

Questioned Cost: A cost that is questioned by the OIG because of: 1) an alleged violation of a provision of a law, regulation, contract, grant, cooperative agreement, or other agreement or document governing the expenditure of funds; 2) a finding that, at the time of the audit, such cost is not supported by adequate documentation; or 3) a finding that the expenditure of funds for the intended purpose is unnecessary or unreasonable.

Recommendation That Funds be Put to Better Use: Recommendation by the OIG that funds could be used more efficiently if management of an entity took actions to implement and complete the recommendation, including: 1) reductions in outlays; 2) deobligation of funds from programs or operations; 3) withdrawal of interest subsidy costs on loans or loan guarantees, insurance, or bonds; 4) costs not incurred by implementing recommended improvements related to the operations of the entity, a contractor, or grantee; 5) avoidance of unnecessary expenditures noted in pre-award reviews of contract or grant agreements; or 6) any other savings that specifically are identified.

Supervised Release: Court-monitored supervision upon release from incarceration.

Unsupported Cost: A cost that is questioned by the OIG because the OIG found that, at the time of the audit, the cost was not supported by adequate documentation.

Appendix 3

Evaluation and Inspections Division Reports

April 1, 2007 – September 30, 2007

Coordination of investigations by the Department's Violent Crime Task Forces

Review of the Department's reporting procedures for loss of sensitive electronic information

ATF's National Firearms Registration and Transfer Record

ATF's investigative operations at gun shows

Health, safety, and security conditions in the H. Carl Moultrie I Courthouse space utilized by the USMS for the District of Columbia Superior Court

The USMS judicial security process

Appendix 4

Audit Division Reports

April 1, 2007 – September 30, 2007

INTERNAL AND EXTERNAL AUDIT REPORTS

Audit of the Department's IT Studies, Plans, and Evaluations

Compliance with Standards Governing CODIS Activities at the Denver Police Department Crime Laboratory, Denver, Colorado

Compliance with Standards Governing CODIS Activities at the Metropolitan Forensic Science Center, Albuquerque, New Mexico

Compliance with Standards Governing CODIS Activities at the Missouri State Highway Patrol Crime Laboratory Division, Jefferson City, Missouri

Compliance with Standards Governing CODIS Activities at the Richland County Sheriff's Department DNA Laboratory, Columbia, South Carolina

Compliance with Standards Governing CODIS Activities at the West Virginia State Police Crime Laboratory, South Charleston, West Virginia

Compliance with Standards Governing CODIS Activities at the Charlotte-Mecklenburg Police Crime Laboratory, Charlotte, North Carolina

Compliance with Standards Governing CODIS Activities at the Joseph A. Jachimczyk Forensic Center, Harris County Medical Examiner, Houston, Texas

Compliance with Standards Governing CODIS Activities at the Oklahoma Central Regional Crime Laboratory, Oklahoma State Bureau of Investigation, Oklahoma City, Oklahoma

Compliance with Standards Governing CODIS Activities at the Oklahoma City Police Department, Oklahoma City, Oklahoma

The Department's Conference Expenditures

Follow-up Audit of the FBI's Efforts to Hire, Train, and Retain Intelligence Analysts

Follow-up Audit of the Terrorist Screening Center

Identification and Review of the Department's Major IT Systems Inventory

Independent Evaluation of ATF Headquarters' Network Infrastructure System Pursuant to FISMA for FY 2006

Independent Evaluation of ATF's Information Security Program Pursuant to FISMA for FY 2006

Independent Evaluation of the DEA's Information Security Program Pursuant to FISMA for FY 2006

Independent Evaluation of the FBI's Information Security Program Pursuant to FISMA for FY 2006

Independent Evaluation of the FBI's System Security Database Pursuant to FISMA for FY 2006

Independent Evaluation of the Follow-up Review of JMD's Information Security Oversight Program Pursuant to FISMA for FY 2006

Independent Evaluation of JMD's Cyber Security Assessment and Management Trusted Agent Sensitive but Unclassified System Pursuant to FISMA for FY 2006

Independent Evaluation of JMD's Cyber Security Assessment and Management Trusted Agent Secret System Pursuant to FISMA for FY 2006

COPS' Grant Awarded to the San Juan Southern Paiute Tribe, Tuba City, Arizona

COPS' Grant Awarded to the Village of Maxwell, New Mexico

COPS' Homeland Security Overtime Program Grant Awarded to the City of Philadelphia Police Department, Philadelphia, Pennsylvania

OJP BJA Correctional Facilities on Tribal Lands Program Grant Awarded to the Salt River Pima-Maricopa Indian Community, Scottsdale, Arizona

OJP BJA Mississippi Automated System Project Grants Awarded to the University of Southern Mississippi, Hattiesburg, Mississippi

OJP Forensic Casework DNA Backlog Reduction Program Cooperative Agreements Awarded to the Texas Department of Public Safety, Austin, Texas

OJP OVC Exploitation and Trafficking Grant Awarded to the Boat People S.O.S., Inc., Falls Church, Virginia

OJP OVC Services for Trafficking Victims Discretionary Grant Program Cooperative Agreement Awarded to the Refugee Women's Network, Inc., Decatur, Georgia

OJP OJJDP Grants Awarded to the Cal Ripken, Sr. Foundation Community Baseball/Softball Program, Baltimore, Maryland

OJP Regional Information Sharing Systems Grant Awarded to the California Department of Justice, Sacramento, California

OJP Services for Trafficking Victims Discretionary Grant Program Cooperative Agreements Awarded to the Mosaic Family Services, Dallas, Texas

OJP Services for Trafficking Victims Discretionary Grant Program Cooperative Agreements Awarded to the YMCA of the Greater Houston Area, Houston, Texas

OJP Southwest Border Prosecution Initiative Funding Received by the County of El Paso, Texas

OJP Southwest Border Prosecution Initiative Funding Received by the Maricopa County Attorney's Office, Phoenix, Arizona

OJP Southwest Border Prosecution Initiative Funding Received by the San Diego County District Attorney's Office, San Diego, California

OJP OVW Grants Administered by Anishinabe Legal Services, Inc., Cass Lake, Wisconsin

OVW Grant Awarded to the West Virginia Division of Criminal Justice Services Rural Domestic Violence and Child Victimization Enforcement, Charleston, West Virginia

Sentinel Audit III: Status of the FBI's Case Management System

Superfund Activities in the ENRD for FYs 2004 and 2005

Survey of Internal Control Procedures Over Department Grant Funds Administered by the University of Southern Mississippi

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Poarch Band of Creek Indians, Atmore, Alabama

Survey of Internal Control Procedures Over Department Grant Funds Administered by Proctor Hospital, Peoria, Illinois

Survey of Internal Control Procedures Over Department Grant Funds Administered by Teen Challenge Illinois, Decatur, Illinois

Survey of Internal Control Procedures Over Department Grant Funds Administered by Barron County Restorative Justice Programs, Inc., Rice Lake, Wisconsin

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Oklahoma Native American Domestic Violence Coalition, Oklahoma City, Oklahoma

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Salt River Pima-Maricopa Indian Community, Scottsdale, Arizona

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Junior Achievement Worldwide, Colorado Springs, Colorado

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Crow Creek Sioux Tribe, Fort Thompson, South Dakota

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Citizens Crime Commission of the Delaware Valley, Philadelphia, Pennsylvania

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Father's Day Rally Committee, Inc., Philadelphia, Pennsylvania

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Town of Newport, Delaware

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Northwest Bronx Community and Clergy Coalition, New York, New York

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Latino Pastoral Action Center, New York, New York

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Office of the Commonwealth's Attorney, Lynchburg, Virginia

Survey of Internal Control Procedures Over Department Grant Funds Administered by Street Law, Inc., Silver Spring, Maryland

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Washington Village Pigtown Neighborhood Planning Council, Inc., Baltimore, Maryland

Survey of Internal Control Procedures Over Southwest Border Prosecution Initiative Grant Funds Administered by the El Paso County, Texas, District Attorney

Survey of Internal Control Procedures Over Technology Improvement Grant Funds Administered by the Middle Rio Grande Development Council, Carrizo Springs, Texas

Survey of Internal Control Procedures Over the Handling of Case Receipts for Department Grant Funds Administered by the Tallapoosa Drug Intervention Program, Cartersville, Georgia

Survey of Internal Control Procedures Over the Handling of Receipts for Department Grant Funds Administered by the DeKalb County, Georgia, Drug Court

Survey of Internal Control Procedures Over Department Grant Funds Administered by the University of South Carolina's Campus Health and Violence Prevention Program, Columbia, South Carolina

The USMS's Workforce Planning and Management

Use of Equitable Sharing Revenues by the Boulder County Drug Task Force, Boulder, Colorado

Use of Equitable Sharing Revenues by the Colorado State Patrol, Lakewood, Colorado

Use of Equitable Sharing Revenues by the Fayette County, Georgia, Sheriff's Office

SINGLE AUDIT ACT REPORTS OF DEPARTMENT OF JUSTICE ACTIVITIES

April 1, 2007 – September 30, 2007

Alfred University, Alfred, New York

City of Atlantic City, New Jersey

City of Bell Gardens, California

City of Chelsea, Massachusetts

City of Dunkirk, New York

City of East Orange, New Jersey

City of Flint, Michigan

City of Georgetown, Kentucky

City of Gulfport, Mississippi

City of Jackson, Mississippi

City of Jersey City, New Jersey

City of King City, California

City of Lynwood, California

City of Montebello, California

City of Moreno Valley, California

City of New Rochelle, New York

City of New York, New York

City of Perris, California

City of Poughkeepsie, New York

City of Riverside, California

City of Susanville, California

City of Vallejo, California

Commonwealth of Kentucky, FY 2004

Commonwealth of Kentucky, FY 2005

Commonwealth of Massachusetts, Boston, Massachusetts, FY 2004

Commonwealth of Massachusetts, Boston, Massachusetts, FY 2005

Commonwealth of Puerto Rico, Office of Youth Affairs, San Juan, Puerto Rico

Council of Juvenile Correctional Administrators, Inc., Braintree, Massachusetts

County of Los Angeles, California

County of Santa Clara, San Jose, California

Crawford County, Van Buren, Arkansas

Department of Corrections, Lansing, Michigan

Department of Human Services, FKA Family Independence Agency, Lansing, Michigan

Department of Justice, San Juan, Puerto Rico

Eastern Kentucky University, Richmond, Kentucky

Fuller Theological Seminary, Pasadena, California

Hogar Crea, Inc., Saint Just, Puerto Rico

Hopland Band of Pomo Indians, Hopland, California

Institute of Forensic Sciences, San Juan, Puerto Rico

Inter-Tribal Council of California, Inc., Sacramento, California

I-Safe America, Inc., Carlsbad, California

Karuk Tribe of California, Happy Camp, California

LaJolla Bank of Luiseno Indians, Pauma Valley, California

Little River Band of Ottawa Indians, Manistee, Michigan

Massachusetts Mental Health Institute, Boston, Massachusetts

Mississippi Institutions of Higher Learning, Jackson, Mississippi

Narragansett Indian Tribe Special Revenue Funds, Charlestown, Rhode Island

National Association of State Fire Marshals, Albany, New York

National Juvenile Detention Association, Inc., Richmond, Kentucky

New York City Gay and Lesbian Anti-Violence Project, Inc., New York, New York

New York University, New York, New York

Nihonmachi Legal Outreach, San Francisco, California

Oregon Museum of Science and Industry, Portland, Oregon

Pennyrile Narcotics Task Force, Hopkinsville, Kentucky

Southeast Uplift Neighborhood Program, Inc., Portland, Oregon

State of Arkansas, Little Rock, Arkansas

State of California, Sacramento, California

State of Mississippi, Jackson, Mississippi

State of Rhode Island and Providence Plantations, Providence, Rhode Island

Table Mountain Rancheria Band of Indians, Friant, California

Tallahatchie County, Charleston, Mississippi

The Fortune Society, Inc., New York, New York

The General Hospital Corporation, Boston, Massachusetts

Town of Apple Valley, California

Town of Lincoln, Rhode Island

Town of Littleton, Massachusetts

University of California, Oakland, California

University of Massachusetts, Shrewsbury, Massachusetts

University of Southern California, Los Angeles, California

Wallowa County, Enterprise, Oregon

Audit Division Reports

April 1, 2007 — September 30, 2007

Quantifiable Potential Monetary Benefits

Audit Report	Questioned Costs	Unsupported Costs	Funds Put to Better Use
Alfred University, Alfred, New York	$258,922	$258,922	
City of East Orange, New Jersey	$400,000	$400,000	
City of Georgetown, Kentucky	$7,641		
City of Jackson, Mississippi	$13,088	$13,088	
City of Montebello, California	$256,943		
City of Moreno Valley, California	$85,322	$85,322	
City of New Rochelle, New York	$329,382	$329,382	
City of New York, New York	$1,596,115	$1,596,115	
Commonwealth of Kentucky, FY 2004	$393,864	$388	
Commonwealth of Kentucky, FY 2005	$407,192		
Commonwealth of Massachusetts, Boston, Massachusetts, FY 2004	$2,046,555	$1,492,263	
Commonwealth of Massachusetts, Boston, Massachusetts, FY 2005	$5,854		
Commonwealth of Puerto Rico, Office of Youth Affairs, San Juan, Puerto Rico	$297,854		
COPS Grant Awarded to the San Juan Southern Paiute Tribe, Tuba City, Arizona	$224,997	$224,997	
COPS Grant Awarded to the Village of Maxwell, New Mexico	$160,366	$66,001	
COPS Homeland Security Overtime Program Grant Awarded to the City of Philadelphia Police Department, Philadelphia, Pennsylvania	$1,203,773	$1,203,773	
Department of Human Services, FKA Family Independence Agency, Lansing, Michigan	$4,085,566	$183,644	
The Department's Conference Expenditures			$225,117

Quantifiable Potential Monetary Benefits

Audit Report	Questioned Costs	Unsupported Costs	Funds Put to Better Use
Eastern Kentucky University, Richmond, Kentucky	$31,109		
OJP BJA Mississippi Automated System Project Grants Awarded to the University of Southern Mississippi, Hattiesburg, Mississippi	$3,198,625		
OJP Forensic Casework DNA Backlog Reduction Program Cooperative Agreements Awarded to the Texas Department of Public Safety, Austin, Texas	$924,373	$924,373	
OJP OVC Exploitation and Trafficking Grant Awarded to the Boat People S.O.S., Inc., Falls Church, Virginia	$716,512	$567,918	
OJP OVC Services for Trafficking Victims Discretionary Grant Program, Cooperative Agreement Awarded to the Refugee Women's Network, Inc., Decatur, Georgia	$15,788		$97,686
OJP OJJDP Grants Awarded to the Cal Ripken, Sr. Foundation Community Baseball/Softball Program, Baltimore, Maryland	$152,403	$55,055	$18,646
OJP Services for Trafficking Victims Discretionary Grant Program Cooperative Agreements Awarded to the Mosaic Family Services, Dallas, Texas	$41,318	$41,318	
OJP Services for Trafficking Victims Discretionary Grant Program Cooperative Agreements Awarded to the YMCA of the Greater Houston Area, Houston, Texas	$21,120	$21,120	
OJP Southwest Border Prosecution Initiative Funding Received by the County of El Paso, Texas	$3,891,196	$3,891,196	
OJP Southwest Border Prosecution Initiative Funding Received by the Maricopa County Attorney's Office, Phoenix, Arizona	$193,357	$176,948	$10,000

Quantifiable Potential Monetary Benefits

Audit Report	Questioned Costs	Unsupported Costs	Funds Put to Better Use
OJP Southwest Border Prosecution Initiative Funding Received by the San Diego County District Attorney's Office, San Diego, California	$288,041		
OJP OVW Grants Administered by Anishinabe Legal Services, Inc., Cass Lake, Wisconsin	$439,204	$418,154	
OVW Grant Awarded to the West Virginia Division of Criminal Justice Services Rural Domestic Violence and Child Victimization Enforcement, Charleston, West Virginia	$37,328	$11,256	
Southeast Uplift Neighborhood Program, Inc., Portland, Oregon	$1,982	$1,937	
State of Arkansas, Little Rock, Arkansas	$124,086		
Tallahatchie County, Charleston, Mississippi	$28,896	$28,896	
Town of Lincoln, Rhode Island	$32,130		
Use of Equitable Sharing Revenues by the Boulder County Drug Task Force, Boulder, Colorado	$88,352		
Use of Equitable Sharing Revenues by the Colorado State Patrol, Lakewood, Colorado	$135,571		
Total	***$22,134,825***	***$11,992,066***	***$351,449***

Appendix 5

Reporting Requirements Index

The IG Act specifies reporting requirements for semiannual reports. The requirements are listed below and indexed to the applicable pages.		
IG Act References	**Reporting Requirements**	**Page**
Section 4(a)(2)	Review of Legislation and Regulations	40
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	7-39
Section 5(a)(2)	Significant Recommendations for Corrective Actions	7-38
Section 5(a)(3)	Prior Significant Recommendations Unimplemented	43-44
Section 5(a)(4)	Matters Referred to Prosecutive Authorities	19-20, 24-27, 29-32, 34-35, 38
Section 5(a)(5)	Refusal to Provide Information	None
Section 5(a)(6)	Listing of Audit Reports	48-55
Section 5(a)(7)	Summary of Significant Reports	7-38
Section 5(a)(8)	Audit Reports – Questioned Costs	42
Section 5(a)(9)	Audit Reports – Funds to Be Put to Better Use	41
Section 5(a)(10)	Prior Audit Reports Unresolved	43
Section 5(a)(11)	Significant Revised Management Decisions	None
Section 5(a)(12)	Significant Management Decisions with which the OIG Disagreed	None

Report Waste, Fraud, Abuse, or Misconduct

To report allegations of waste, fraud, abuse, or misconduct in Department of Justice programs, send complaints to:

Office of the Inspector General
U.S. Department of Justice

Investigations Division
950 Pennsylvania Avenue, NW
Room 4706
Washington, DC 20530

E-mail: oig.hotline@usdoj.gov
Hotline: (800) 869-4499
Hotline fax: (202) 616-9881

Report Violations of Civil Rights and Civil Liberties

Individuals who believe that a Department of Justice employee has violated their civil rights or civil liberties may send complaints to:

Civil Rights and Civil Liberties Complaints
Office of the Inspector General

U.S. Department of Justice
950 Pennsylvania Avenue, NW
Room 4706
Washington, DC 20530

E-mail: inspector.general@usdoj.gov
Hotline: (800) 869-4499
Hotline fax: (202) 616-9898

U.S. Department of Justice
Office of the Inspector General