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

Semiannual Report to Congress

April 1, 2011 - September 30, 2011

Online Report Availability

OIG audit, evaluation, inspection, and special review reports as well as investigations press releases are available at www.justice.gov/oig.

Information about the federal Inspector General community is 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

Automatic E-Mail Updates

The Office of the Inspector General (OIG) offers a free e-mail subscription service that provides automatic notifications by e-mail when new reports or other information is posted to the OIG website.

To receive e-mail notifications of additions to the OIG website, go to the OIG website at www.justice.gov/oig, click on "Sign Up For E-mail Updates," and then click the link labeled "Start, Change, or Cancel Your Subscription." You will be asked to provide the e-mail address where you want the notifications to be sent. You can elect to receive notifications for all reports and documents when they are added to the OIG website or you can elect to receive notifications for only certain types of OIG reports and documents. At any time, you can change your e-mail address, modify your password, add or delete subscriptions, or remove your e-mail address from this service.

Message from the Acting Inspector General

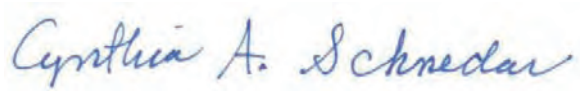
This semiannual report summarizes the work of the Office of the Inspector General (OIG) from April 1, 2011, through September 30, 2011. Our audits, inspections, evaluations, investigations, and reviews during this period addressed many of the top management and performance challenges facing the Department of Justice (Department).

In the current climate of lean economic times and budget limitations, the OIG continues to focus oversight on areas where the Department can save money and enhance efficiency. Of particular importance, we are continuing our oversight of several of the Department's information technology development projects. During the past six months, we released a report examining the Department's $1 billion project to upgrade and consolidate the six accounting systems used by the Department and its components into the new Unified Financial Management System. This report found that the project has experienced delays in schedule and an increase in costs, and that the original scope of the project has been significantly reduced. We are continuing our work on the Federal Bureau of Investigation's (FBI) planned $451 million dollar project to develop the Sentinel case management project and on the Department's development of the planned $1.2 billion Integrated Wireless Network to facilitate communication among federal law enforcement officials in different agencies.

We also looked at other areas where the Department can implement cost savings or improve efficiency, including a report identifying ways that the U.S. Marshals Service could improve its management of complex assets that are seized in financial crimes and a report identifying steps the Department can take to minimize conference-related costs.

OIG reviews in other areas included a review of the FBI's ability to address the threat of cyber intrusions in which we identified steps the FBI could take to enhance its investigations of these incidents. We also released an audit report finding that the FBI Laboratory had achieved a significant accomplishment by reducing its backlog of convicted offender, arrestee, and detainee DNA samples to a manageable monthly workload. We are continuing our review of issues raised concerning the Department's actions in the implementation of the gun trafficking investigation known as Operation Fast and Furious. And importantly, our Investigations Division continues to investigate significant allegations of criminal or administrative misconduct related to Department personnel or programs.

We believe that our work in these and other matters will help ensure that the Department pursues its mission in a manner that is effective, efficient, and just. I want to thank the Department and Congress for their continued support, and I particularly want to thank the OIG employees for their hard work and dedication. Together, we are achieving the important OIG mission of improving the critical functions of the Department of Justice.

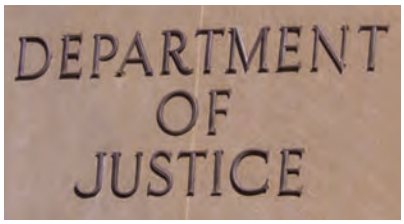


Cynthia A. Schnedar
Acting Inspector General
October 31, 2011

Table of Contents

Table of Contents

Highlights of OIG Activities



The following summaries highlight some of the Office of the Inspector General's (OIG) audits, evaluations, inspections, special reviews, and investigations, which are discussed further in this report. As the highlights illustrate, the OIG continues to conduct wide-ranging oversight of Department of Justice (Department) programs and operations.

Statistical Highlights

April 1, 2011 - September 30, 2011	
Allegations Received by the Investigations Division	5,985
Investigations Opened	174
Investigations Closed	210
Arrests	51
Indictments/Informations	50
Convictions/Pleas	52
Administrative Actions	109
Monetary Recoveries[1]	$15,262,003
Audit Reports Issued	52
Questioned Costs	$2,560,422
Recommendations for Management Improvements	225
Single Audit Act Reports Issued	14
Questioned Costs	$189,784
Recommendations for Management Improvements	53

1 Includes civil, criminal, non-judicial fines, restitutions, recoveries, assessments, penalties, and forfeitures.

Audits, Evaluations, Inspections, and Special Reviews Highlights

Examples of OIG audits, evaluations, inspections, and special reviews completed during this semiannual reporting period are:

- **Administration of Complex Asset Team Management and Oversight.** The OIG issued a report finding significant deficiencies in how the U.S. Marshals Service (USMS) managed complex assets, including those seized as part of financial crime cases, between 2005 and 2010. Since 2005, the Complex Asset Team — responsible for helping USMS district offices manage and dispose of unique and complicated assets that have been seized or forfeited to the federal government — had disposed of over $130 million in complex assets, including business and financial interests seized during investigations into several multi-million dollar financial crimes perpetrated by individuals including Ponzi-scheme operator Bernard Madoff, investment lawyer Scott Rothstein, banker and political fundraiser Hassan Nemazee, and organized crime figure James Galante. The OIG audit found that the USMS's lack of pre-seizure planning exposed the government to unnecessary risk, such as seizing assets with significant liabilities or limited equity, or becoming involved in protracted litigation with third parties who have interests in the assets. The audit report made 20 recommendations to help the USMS and the Justice Management Division (JMD) better manage and account for seized and forfeited complex assets. The USMS concurred with the recommendations and has already begun to implement recordkeeping, reporting, and valuation procedural improvements.

- Efforts to Combat National Security Cyber Threats. The OIG conducted a review of the Federal Bureau of Investigation's (FBI) efforts to develop the National Cyber Investigative Joint Task Force (NCIJTF), an FBI-led, multi-agency task force responsible for ensuring that the U.S. government coordinates its efforts to combat national security cyber intrusions, and the capabilities of FBI field offices to investigate national security cyber intrusion cases. The audit found that the FBI has completed many of the interim goals for the NCIJTF. In addition to developing an operational plan for the NCIJTF, the FBI incorporated many intelligence community and law enforcement agencies in day-to-day NCIJTF operations, formed threat focus cells comprised of NCIJTF participants' expertise to target specific cyber threats, and had some operational successes in mitigating cyber threats against the United States. The NCIJTF could improve its capabilities to defend against cyber attacks by sharing relevant information about cyber threats among the task force's partner agencies. In addition, the FBI could improve the capabilities of its field offices so that new cyber agents are equipped to assume responsibility of a national security intrusion investigation. The OIG made several recommendations to help the FBI implement the NCIJTF and strengthen its cadre of field agents assigned to investigate national security cyber intrusions, and the FBI concurred with the recommendations.

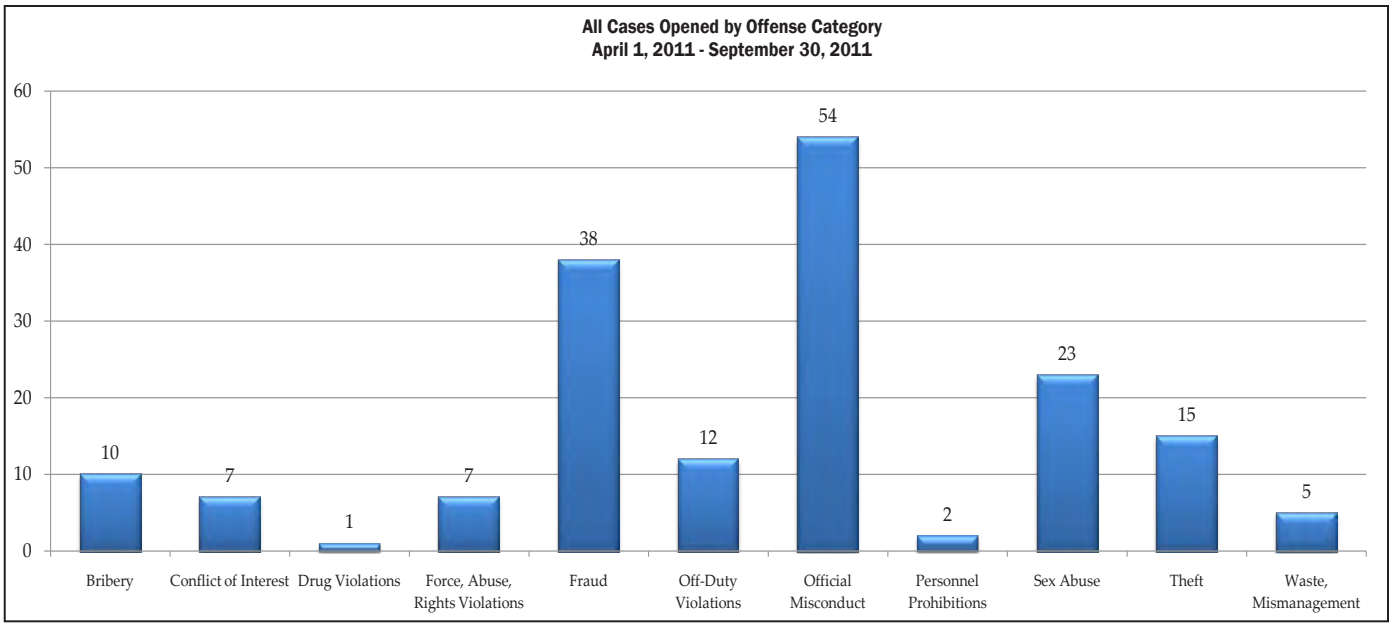
- Convicted Offender, Arrestee, and Detainee DNA Backlog. The OIG examined the FBI's efforts to eliminate its backlog of DNA samples collected from federal convicted offenders, federal arrestees, and non-U.S. citizen detainees, and determined that the FBI has effectively eliminated its backlog to a manageable monthly workload. In December 2009, the FBI Laboratory reported a backlog of over 312,000 convicted offender, arrestee, and detainee DNA samples waiting to be processed. The OIG audit determined that as of May 2011, the FBI had reduced its backlog to approximately 14,000 samples by hiring additional personnel and contractors, using high-throughput robotics, implementing software for a semi-automated review of DNA profiles after completion of analysis, and reconfiguring laboratory space for more efficient processing. However, the OIG audit found that the FBI Laboratory lacked documented policies, procedures, and reporting methods to ensure backlog and workload levels are accurately identified and reported. In addition, the FBI Laboratory had over 712,000 DNA samples that required storage, and it anticipates having 1 million samples by the end of the calendar year, which could present storage issues in the future. The OIG made recommendations to assist the FBI in more accurately identifying, reporting, and projecting its convicted offender, arrestee, and detainee DNA sample workload, and to develop a long-term plan to store DNA samples, and the FBI concurred with these recommendations.

Investigative Highlights

As shown in the statistics at the beginning of this section and in the following chart, the OIG investigates many allegations of misconduct involving Department employees, contractors, or grantees who receive Department money. Examples of such investigations are:

- On August 29, 2011, a retired naval officer was found guilty by a jury in the U.S. District Court for the District of

Highlights of OIG Activities



Source: Investigations Data Management System

Columbia for filing a false claim with the September 11th Victim Compensation Fund and stealing approximately $151,000 from the government. The evidence at trial showed that the retired naval officer was stationed at the Pentagon on September 11, 2001, and claimed that he was injured during the terrorist attack on the building. He claimed the injuries that he suffered prevented him from playing competitive lacrosse and doing home improvement work. The evidence showed that the retired naval officer continued to play competitive lacrosse, ran the New York City Marathon in November 2001, and falsified documents submitted to the Victim Compensation Fund. The investigation was conducted by the OIG's Fraud Detection Office.

- On August 23, 2011, the mayor of Kinloch, Missouri, Keith Conway, was arrested and pled guilty to charges of wire fraud and theft of funds from a federal program. Kinloch received $90,000 in *American Recovery and Reinvestment Act of 2009* (Recovery Act) funds from an Office of Community Oriented Policing Services (COPS) grant. In entering his guilty plea, the mayor admitted that he used city funds to pay for several luxury items.

- On April 11, 2011, a Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) Special Agent assigned to the Washington Field Division pled guilty to charges of theft of public property, possessing or receiving stolen firearms, false statements, wire fraud, and money laundering. In pleading guilty, the Special Agent admitted that in his official capacity, he converted ATF seizures of firearms, tobacco, and currency to his personal use. Also, the Special Agent admitted that he falsified official ATF documents relating to the disposition of the firearms and made unauthorized sales of tobacco product inventory and retained the proceeds. The Special Agent was subsequently sentenced in the

Eastern District of Virginia to 37 months' imprisonment followed by 2 years of supervised release and ordered to pay $10,210 in restitution as well as forfeiture of $4,860 in recovered government funds. The Special Agent resigned from the ATF. The investigation by the OIG's Washington Field Office was conducted with the assistance of ATF and the City of Hampton, Virginia, Police Department.

- On August 10, 2011, an FBI Supervisory Senior Resident Agent was arrested and pled guilty on charges of making false statements. The Supervisory Senior Resident Agent admitted in pleading guilty that in 2010 he prepared a false evidence inventory and receipt form claiming that he had removed cash seized in a drug investigation in 2009 from FBI evidence and then placed it back into evidence at a local drug task force office. He admitted that he forged the signatures of two law enforcement officers as witnesses of the alleged transfer of cash on the evidence inventory and receipt form. The Supervisory Senior Resident Agent is no longer an FBI employee.

- On May 3, 2011, the Federal Express Corporation agreed to pay $8 million to settle allegations that the company and its affiliates violated the federal *False Claims Act* related to a contract with the government. In the wake of the 2001 terrorist attacks in New York and Washington, D.C., Federal Express couriers used "delivery exception codes" to reflect that increased security measures at government facilities were causing delays in the timely delivery of overnight Federal Express packages. A joint investigation conducted by the Department's OIG Fraud Detection Office, the General Services Administration OIG, and the Department of Agriculture OIG determined that, even after heightened security measures subsided or became routine procedures for entering government locations, Federal Express couriers used "delivery exception codes" in order to excuse their own failures to deliver Priority Overnight packages by the specified time, thus avoiding the obligation to reimburse government customers under the company's money-back-guarantee policy.

- On September, 1, 2011, a former Bureau of Prisons (BOP) contractor and her husband were arrested and pled guilty to conspiracy to commit false statements relating to health care matters. The BOP contractor and her husband were operators of a company funded in part by Medicaid and which provided services to persons with developmental disabilities. In pleading guilty, the BOP contractor, who was a licensed psychologist working in the Education Department of a BOP facility in Texas, admitted that she obtained the personally identifiable information of inmates and used this information in a scheme to defraud Medicaid. In total, the BOP contractor and her husband fraudulently obtained $1,820,359 from the Texas Medicaid program. BOP had previously terminated the contract. The investigation was conducted by the OIG's Dallas Field Office and the Texas State Attorney General's Office, Medicaid Fraud Control Unit.

- On September 12, 2011, the U.S. District Court for the Southern District of New York ordered Mario Mastellone to pay a civil judgment of $3,241,367 for violating the *False Claims Act*. Following the September 11, 2001, terrorist attacks on New York, Mastellone submitted an application to the Department of Justice September 11th Victim Compensation Fund. In his application, he claimed

that he was totally and permanently disabled in connection with the terrorist attacks. In June 2008, following a joint investigation by the OIG's Fraud Detection Office and the New York Field Office, Mastellone pled guilty to stealing $1,076,789 from the fund and was sentenced to 30 months' incarceration followed by 3 years of supervised release. The civil judgment against Mastellone ordered him to pay triple the amount stolen from the government.

- On April 1, 2011, an FBI financial analyst assigned to the FBI Tampa Division in Tampa, Florida, was arrested and pled guilty to charges of theft of government property. In pleading guilty, the financial analyst admitted submitting fraudulent requests for disbursement of government funds through the FBI Tampa Division draft office. The financial analyst was sentenced in the Middle District of Florida to 60 months' probation and was ordered to pay $1,190 in restitution. The financial analyst retired from the FBI. The investigation was conducted by the OIG's Miami Field Office.

- In our March 2011 *Semiannual Report to Congress*, the OIG reported on an investigation that led to the arrest and guilty plea of a former USMS administrative officer to theft of $104,000 in government funds. The former administrative officer admitted that she unlawfully used a USMS credit card for personal expenses, created a fictitious employee in the USMS payroll system and submitted falsified time and attendance records for the employee, facilitated the issuance of checks, and disguised the theft with fraudulent business invoices. Prior to this investigation, the former administrative officer had left the USMS in November 2008 and obtained employment with the Drug Enforcement Administration (DEA) in a similar capacity. During this reporting period, the former USMS administrative officer was sentenced in the U.S. District Court for the District of Columbia, Washington, D.C., to 21 months' imprisonment followed by 36 months' supervised release and ordered to pay $104,000 in restitution.

- In our March 2011 *Semiannual Report to Congress*, the OIG reported on an investigation that led to the arrest of a former Supervisory Deputy U.S. Marshal, previously assigned to the USMS Northern District of Illinois, Chicago Office, based on an indictment returned in the Northern District of Illinois charging him with making false statements to the OIG. The investigation by the OIG's Chicago Field Office determined that the Supervisory Deputy U.S. Marshal provided criminal history, motor vehicle, and driver license information obtained from restricted law enforcement databases to a friend who was under investigation by the FBI for staging fake accidents to collect insurance proceeds. The Supervisory Deputy U.S. Marshal provided false and misleading information regarding these actions during his OIG interview. During this reporting period, the Supervisory Deputy U.S. Marshal was sentenced to 36 months' probation and fined $5,000 pursuant to his guilty plea to charges of making false statements to the OIG. The Supervisory Deputy U.S. Marshal retired from the USMS.

- In our September 2010 *Semiannual Report to Congress*, the OIG reported on an investigation that led to the arrest of an FBI Special Agent on charges of wire fraud, bank fraud, and bankruptcy fraud charges. The investigation by the OIG's Miami Field Office developed evidence that the Special Agent provided false information to obtain mortgage

loans. In his mortgage applications, the Special Agent falsely claimed that he was employed by an alleged music company. Additionally, the Special Agent secured a home equity line of credit. The FBI Special Agent filed for bankruptcy in July 2009, and he failed to include properties the Special Agent owned or transferred on the bankruptcy application. During this reporting period, he was found guilty at trial on 15 counts of wire fraud and 3 counts of bankruptcy fraud and sentenced in the Middle District of Tennessee to 48 months' incarceration followed by 36 months' supervised release and was ordered by the court to pay $675,143 in restitution.

Ongoing Work

This report also describes ongoing OIG reviews, including reviews of:

- The ATF's firearms trafficking investigation known as Operation Fast and Furious, and other investigations with similar objectives, methods, and strategies.
- The Civil Rights Division's enforcement of civil rights laws by its Voting Section.
- The FBI's management of terrorist watchlist nominations and encounters with watchlisted subjects, which includes evaluating the effectiveness of the FBI's initiatives to ensure the accuracy, timeliness, and completeness of its watchlisting practices.
- The Department's role in the transfer of foreign national inmates incarcerated in federal prisons through the international prisoner treaty transfer program.
- The FBI and National Security Division's (NSD) efforts to appropriately handle and coordinate shared responsibilities for identifying, investigating, and prosecuting persons and entities who provide financial support to terrorist organizations.
- The FBI's ongoing development and implementation of the Sentinel information technology project, which is intended to upgrade the FBI's electronic case management system and provide the FBI with an automated workflow process.
- The Department's Integrated Wireless Network program to evaluate the Department's cost, schedule, and performance and assess progress in resolving concerns identified in our previous audit.
- The FBI's activities under Section 702 of the *FISA Amendments Act of 2008*.
- The FBI's use of national security letters, Section 215 orders, and pen register and trap-and-trace authorities under the *Foreign Intelligence Surveillance Act of 1978* (FISA) from 2007 through 2009.

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, ATF, BOP, DEA, U.S. Attorney's Office (USAO), USMS, 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 the Atlanta, Chicago, Dallas, Denver, Philadelphia, San Francisco, and Washington, D.C., areas. Its Financial Statement Audit Office and Computer Security and Information Technology Audit Office are located in Washington, D.C., along with Audit Headquarters. Audit Headquarters consists of the immediate office of the Assistant Inspector General for Audit, Office of Operations, Office of Policy and Planning, and Advanced Audit Techniques.

- **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 Investigations Division has smaller, area offices in Atlanta, Boston, Detroit, El Paso, Houston, New Jersey, San Francisco, and Tucson. The Fraud Detection Office is co-located with the Washington Field Office. 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.

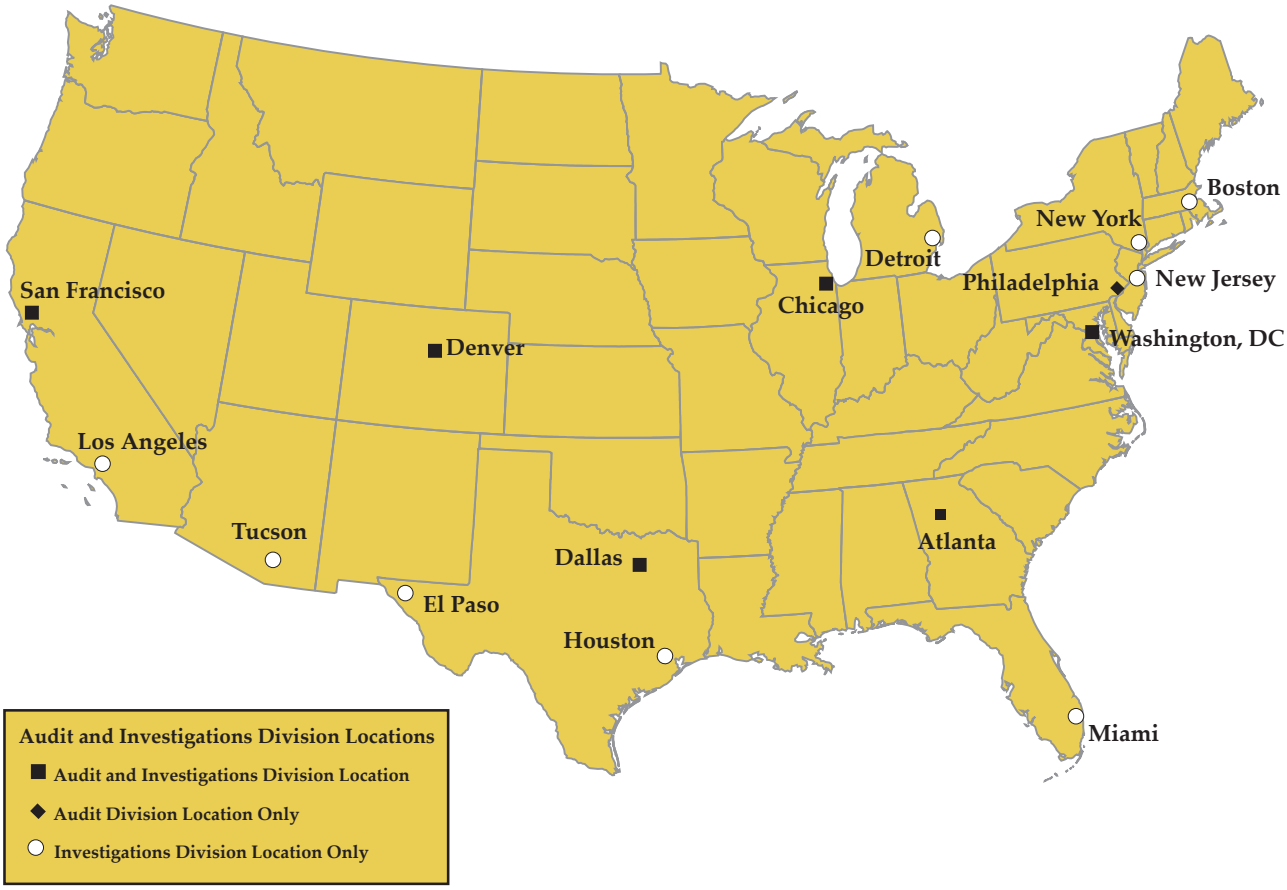
- **Oversight and Review Division** blends the skills of attorneys, investigators, program analysts, and paralegals to conduct special reviews and investigations of sensitive allegations involving Department employees and operations.

- **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, records management, 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 map below shows the locations for the Audit and Investigations Divisions.



The OIG has a nationwide workforce of approximately 447 special agents, auditors, inspectors, attorneys, and support staff. For Fiscal Year (FY) 2011, the OIG direct appropriation was $84 million, and the OIG earned an additional $4 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, 2011, through September 30, 2011, is to be submitted no later than October 31, 2011, to the Attorney General for his review. The Attorney General is required to forward the report to Congress no later than November 30, 2011, along with information on the Department's position on 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.justice.gov/oig.

Multicomponent

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

Reports Issued

Unified Financial Management System

The OIG issued a report on the status of the Department's implementation of the Unified Financial Management System (UFMS), a project to upgrade and consolidate six accounting systems used by the Department and its components. The OIG conducted this review of whether the UFMS project was on budget and being implemented according to schedule.

During our review, we found that the scope of the UFMS project had been significantly reduced. As a result of an Office of Management and Budget (OMB) review in 2010, the Department cut 20 percent of the UFMS project budget and will not pursue a single, unified financial system as planned. Rather than a single, unified financial system that previously was envisioned, the Department is planning to operate two financial management systems, UFMS and the Financial Management Information System 2 (FMIS2).

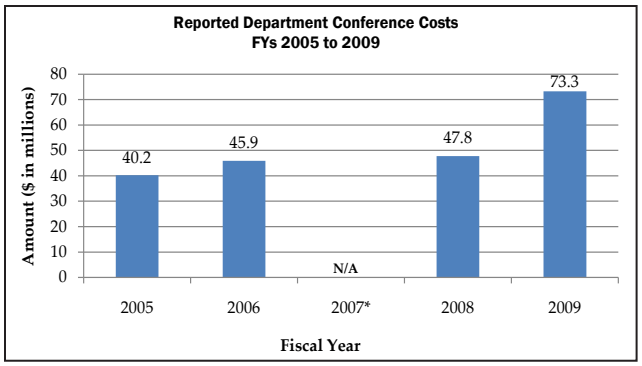
We found that the Department's effort to implement the UFMS project experienced schedule delays and increased costs. In 2002, the UFMS project was expected to take 8 years to implement and cost $357.2 million, which included operation and maintenance coverage until 2012. The Department revised its cost estimate in April 2010 to $1.041 billion, adding an additional 3 years to the completion date, and extending the operation and maintenance coverage to 2021. As a result of the OMB review, the Department reduced UFMS project costs to $851 million.

We found that UFMS has only been implemented at two of the Department's components, the DEA in January 2009 and ATF in October 2010. Following the DEA and ATF implementations, the Department will implement UFMS at the USMS and FBI. We believe that significant challenges remain with the implementation at the USMS and FBI, because these two components use more antiquated financial management systems than the systems that were in use at the DEA and ATF prior to the implementation of UFMS.

As a result of the changes made to the program by the Department after OMB's review, UFMS will not be implemented at the BOP, Office of Justice Programs (OJP), and the Department's Offices, Boards and Divisions. Instead, these Department components will continue to utilize FMIS2. The possibility remains that UFMS will be implemented at the BOP, OJP, and the Department's Offices, Boards, and Divisions in the future; however, this conversion would be a separate project from the current UFMS project, and this new project would require both OMB approval and additional funding.

Conference Planning and Food and Beverage Costs

The OIG examined 10 Department conferences that cost $4.4 million. Overall, the Department hosted or participated in 1,832 conferences in FYs 2008 and 2009, at a cost of $121 million. This audit follows a 2007 OIG report that identified extravagant costs associated with food and beverages and event planning activities — categories identified as most potentially susceptible to wasteful spending.



Source: Department component expenditures reports

The current audit found that while the Department has instituted conference cost guidance since the 2007 report, individual components are not taking all necessary steps to minimize conference-related costs and eliminate wasteful spending. The audit found that two components, OJP and the Office on Violence Against Women (OVW), spent approximately $600,000 at five conferences to procure event planning services from training and technical assistance providers without demonstrating that these firms offered the most cost effective logistical services. The audit found that neither OJP nor the OVW required event planners to track and report salary and benefit costs. As a result, the congressionally mandated Department conference costs reports did not include over $500,000 of the $600,000 spent on event planning services for the five conferences we examined where training and technical assistance providers were used to plan conferences.

In addition to reviewing event planning services, the audit also reviewed the meals and refreshment charges from the 10 selected conferences. The audit found that some Department components did not minimize conference costs as required by federal and Department guidelines and had incurred costs that appeared extravagant and wasteful.

We also found that because the Department policy limiting meal and refreshment costs did not apply to conferences planned under cooperative agreements — funding vehicles used when components expect to be substantially involved in the work performed — certain components could circumvent meal and refreshment cost limits by funding conferences with cooperative agreements.

The report makes 10 recommendations, including that the Department uses training and technical assistance providers for planning conferences only when it can be demonstrated that it is the most cost-effective method of providing logistical services; that recipients of Department funds for conference planning be required to track their time and activities associated with such services; and conference cost reports provided to Congress include all event planner costs charged to the government. Overall, the Department generally concurred with the OIG recommendations.

After publication of the report, we received additional documents and information concerning the food and beverage costs at one of the ten conferences we reviewed. After further review of the newly provided documentation and information, and after discussions with the hotel that hosted the conference and the Department, we determined that our initial conclusions concerning some of the itemized costs of refreshments at this conference were incorrect. We issued a revised report in October 2011 reflecting the corrected information.

* The Department did not compile conference expenditure reports for FY 2007 because there were no requests from Congress or legislative requirements to compile and report this information.

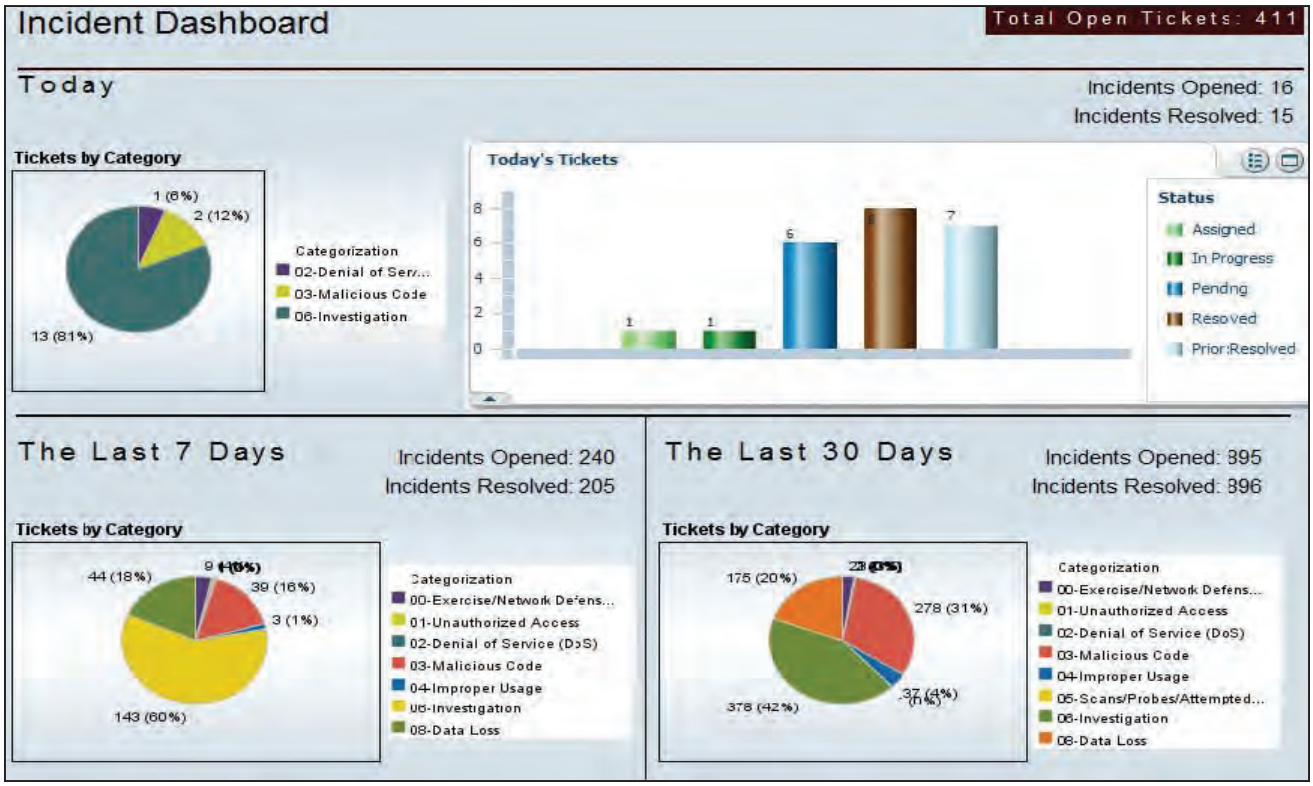
Justice Security Operations Center's Capabilities and Coordination

The OIG reviewed the operations of the Justice Security Operations Center (JSOC), which was established in 2007 to protect the Department's information technology systems from cyber intrusions, attacks, espionage, and other cyber incidents. The audit assessed JSOC's capabilities, and its cooperation and coordination with components and the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT), which provides response support and defense against cyber incidents and attacks for the Executive Branch. In addition to providing cyber incident response planning, training, and assistance to all components, JSOC works with components to prevent, monitor, mitigate, and resolve cyber incidents and attacks on the Department.

The OIG audit found that JSOC has many processes and procedures that appear to provide effective monitoring of network traffic and of information received from components and offices. The audit also found that JSOC reports cyber incidents to US-CERT and coordinates with components, and that components are generally satisfied with JSOC.

However, the OIG also identified needed improvements to JSOC's monitoring and coordination activities. For example, the audit found that JSOC policy allows more time — potentially up to twice as long — for reporting incidents to US-CERT than US-CERT advises, and that JSOC has not developed specific guidance defining when a cyber incident is "widespread," a category of incident that requires more immediate reporting to US-CERT. The audit also found that JSOC's documentation of some cyber incidents is insufficient to enable adequate monitoring and resolution of the incident, and as a result, incidents can remain unresolved for an extended time.

Example of JSOC's Consolidated Incident Dashboard



Source: JSOC

Multicomponent

The audit also concluded that six components have not provided all available information feeds to JSOC, thereby limiting JSOC's ability to monitor cyber activity. Additionally, the audit concluded that the FBI does not report to JSOC incidents that the FBI categorizes as "under investigation," a practice that may prevent JSOC from maintaining a comprehensive view of the network. These limitations on JSOC's monitoring activities potentially increase the Department's vulnerability to cyber intrusion or attack. We recommended that JSOC obtain necessary information feeds and incident reports from all components, including establishing a policy for the periodic reporting of incidents categorized as under investigation, to ensure that it can adequately monitor networks and respond effectively to cyber incidents.

The report made 20 recommendations to improve JSOC's ability to report and manage information pertaining to cyber incidents and enhance the effectiveness of coordination between JSOC and components and offices, and the Department concurred with the recommendations.

Processing of Clemency Petitions

This audit examined the Department's processing of clemency petitions. The Department assists the President in the exercise of his constitutional power to grant clemency by providing advice and counsel on which to base his decisions. Requests for executive clemency are directed to the Office of the Pardon Attorney (OPA), which consults with other Department components, conducts necessary investigations, and prepares recommendations for the Deputy Attorney General, prior to transmittal to the White House for the President's decision.

The audit found that the backlog of pending clemency petitions increased by 92 percent over 6 years, from 2,459 petitions at the beginning of FY 2005 to 4,714 petitions at the end of FY 2010. During this same time, the number of petitions processed by the OPA increased by 61 percent.

In addition, the audit found that, during the audit period, it took on average almost two years to process clemency petitions from the OPA's receipt of the petition to the President's final decision. We determined that a significant cause of the delay in processing clemency petitions was that components often did not respond to the OPA's referrals within the period of time required by the components' internal guidelines or the period of time requested by the OPA. Despite these guidelines, we found the average response time for a component receiving a referral was 124 days (4.1 months) per petition, ranging from 30 days (1 month) to more than 489 days (16.3 months).

Average Referral Response Time Per Petition, FYs 2005 - 2010

Referral Agency	Average Time at Each Agency	Established Timeframe at Each Agency
BOP (Referrals to Wardens Only)	105 days	15 days
USAOs	153 days	30 days
Civil Rights Division	263 days	30 days
FBI	343 days	120 days
Criminal Division	489 days[1]	30 days

1 The average time includes three petitioners who were prosecuted by the Criminal Division's former Counterespionage Section, which is now part of the NSD. We found these to be valid referrals because the referrals occurred during the time that the Counterespionage Section was a part of the Criminal Division and the Criminal Division was the primary prosecuting agency. Nonetheless, if these petitions were removed from our calculation, the average response time for the Criminal Division would be 233 days (7.8 months) per petition.

Although 8 of the 10 components receiving referrals from the OPA have established internal guidelines that require them to respond to the OPA, or to advise the OPA if an unusual delay is anticipated, the OIG found that these components generally did not comply with the 30 day timeframe and did not notify the OPA if additional time was required to provide a response to a referral. In addition, the OPA often did not follow up on outstanding referrals within the 60 days required by internal OPA policy. The OIG recommended that the OPA improve its procedures to ensure timely follow-up with components, processing referrals electronically when appropriate, and ensuring that the OPA's case management system is updated regularly and accurately reflects changes in the status of referrals.

In addition to the average 9.8 months needed for the OPA to complete its initial review and recommendations, we found that petitions also remained pending with the Office of the Deputy Attorney General for an average of 142 days (4.7 months) as that office reviewed the OPA's report and recommendation. The OIG recommended that the Office of the Deputy Attorney General develop policies, procedures, and timeframes for reviewing the OPA's clemency reports and recommendations to help ensure that it responds to the OPA in a timely manner.

While the audit found that it took a total of almost 2 years to process clemency petitions from the OPA's receipt of the petition to the President's final decision, included in that figure was the average of 282 days (9.4 months) that petitions were at the White House awaiting a final decision by the President.

The OIG made 10 recommendations to assist the Department components in processing clemency petitions and referrals in a more efficient manner and in reducing the backlog of pending petitions at the Department. Nine out of ten components included in this audit agreed with the OIG recommendations and the OIG is working with the remaining component to resolve the disagreement.

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. OMB issued guidance to agencies for the FY 2011 FISMA requirements. OMB instructed agency Chief Information Officers, Inspectors General, and Senior Agency Officials for Privacy to report FY 2011 FISMA results to OMB by November 15, 2011.

For FY 2010, the OIG audited the security programs of eight Department components: the U.S. National Central Bureau of INTERPOL (INTERPOL), Executive Office for U.S. Attorneys (EOUSA), OJP, NSD, FBI, ATF, DEA, and JMD. Within these components, we selected for review four classified systems within the DEA, NSD, FBI, and JMD and four sensitive but unclassified systems in the other components: INTERPOL's Envoy System, EOUSA's Case Management Enterprise System, OJP's National Criminal Justice Reference Service, and ATF's National Field Office Case Information System. In these audits, we identified deficiencies in configuration management and security training. We provided 69 recommendations for improving implementation of the Department's information security program and practices for its sensitive but unclassified, classified, and national security systems. The components agreed with our recommendations.

For FY 2011, we are reviewing the security programs for six Department components: the

FBI, JMD, the BOP, USMS, Criminal Division, and the Tax Division. Within these components, we selected for review two classified systems within the FBI. In addition we also selected four sensitive but unclassified systems in the other components: JMD's Endpoint Lifecycle Management System, the BOP's TrueFone System, USMS's Justice Prisoner and Alien Transportation System, the Criminal Division's Justice Consolidated Office Network IIA, and the Tax Division's Tax Office Automation System. The OIG plans to issue reports evaluating each of these systems.

In addition, FISMA requires an annual evaluation of the information security programs and practices of Intelligence Community (IC) agencies, which include the FBI. The Office of the Director of National Intelligence has the responsibility for analyzing, summarizing, and consolidating the IC OIG FISMA reports into one capstone annual report. Therefore, on September 9, 2011, we submitted IC FISMA Metrics Report for the FBI to the Office of the Director of National Intelligence.

Civil Rights and Civil Liberties Complaints

Section 1001 of the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (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 the OIG's implementation of these responsibilities. In August 2011, the OIG issued its 19th report summarizing its Section 1001 activities covering the period from January 1 – June 30, 2011. The report described the number of complaints we received under this section and the status of investigations conducted by the OIG and Department components.

Investigations

The following is an example of a case involving more than one component that the OIG's Investigations Division investigated during this reporting period:

- On May 3, 2011, the Federal Express Corporation agreed to pay $8 million to settle allegations that the company and its affiliates violated the federal *False Claims Act* related to a contract with the government. In the wake of the 2001 terrorist attacks in New York and Washington, D.C., Federal Express couriers used "delivery exception codes" to reflect that increased security measures at government facilities were causing delays in the timely delivery of overnight Federal Express packages. A joint investigation conducted by the Department's OIG Fraud Detection Office, the General Services Administration OIG, and the Department of Agriculture OIG determined that, even after heightened security measures subsided or became routine procedures for entering government locations, Federal Express couriers used "delivery exception codes" in order to excuse their own failures to deliver Priority Overnight packages by the specified time, thus avoiding the obligation to reimburse government customers under the company's money-back-guarantee policy.

Multicomponent

Ongoing Work

Use of Material Witness Warrants

The OIG is reviewing the Department's use of the material witness warrant statute, 18 U.S.C. Section 3144. The review is examining trends in the Department's use of material witness warrants over time, controls over their use, and the Department's treatment of material witnesses in national security cases, including issues such as length of detention, conditions of confinement, and access to counsel. Pursuant to the OIG's responsibility under Section 1001 of the Patriot Act, the review is also addressing allegations of civil rights and civil liberties abuses in the Department's post-September 11th use of the statute in the national security context.

Operation Fast and Furious and Similar Firearms Trafficking Investigations

The OIG is reviewing ATF's firearms trafficking investigation known as Operation Fast and Furious, and other investigations with similar objectives, methods, and strategies. The review is examining the development and implementation of the investigations; the involvement of the Department (including ATF, the Criminal Division, and USAOs) and other law enforcement or government entities in the investigations; the guidelines and other internal controls in place and compliance with those controls during the investigations; and the investigative outcomes.

International Prisoner Treaty Transfer Program

The OIG is reviewing the Department's role in the transfer of foreign national inmates incarcerated in federal prisons through the international prisoner treaty transfer program. The review is assessing the Department's process to approve or deny inmates' requests to serve their sentences in the foreign countries in which they are citizens.

FBI and National Security Division Efforts to Combat Terrorist Financing

The FBI and NSD share responsibility for identifying, investigating, and prosecuting persons and entities who provide financial support to terrorist organizations. The OIG is examining whether the FBI and NSD are appropriately handling these responsibilities and coordinating their efforts.

Internal Controls over Terrorism Reporting

The OIG is conducting a follow-up audit of the Department's internal controls over its terrorism reporting. The audit will determine whether the NSD, EOUSA, and the FBI took appropriate actions to implement the recommendations from the 2007 audit. We are also reviewing whether corrective actions implemented improved the components' ability to gather, track, classify, verify, and report accurate terrorism-related statistics.

Integrated Wireless Network

The OIG is conducting a follow-up audit of the Department's Integrated Wireless Network project to evaluate its cost, schedule, and performance and assess progress in resolving concerns identified in the previous audit. The Integrated Wireless Network is a joint effort of the Department, and the Departments of Homeland Security and the Treasury to provide a secure, interoperable nationwide wireless communications network.

Multicomponent

Administrative Suspension, Debarment, and Other Internal Remedies within the Department

Suspension and debarment actions preclude individuals or entities from participating in government contracts, subcontracts, loans, grants, and other assistance programs. Federal agencies can suspend or debar a party for reasons such as a conviction, an indictment for a criminal offense, or a willful failure to perform to the terms of a contract or grant. The OIG is evaluating the Department's implementation and oversight of suspension, debarment, and other enforcement tools designed to ensure federal agencies award federal funding only to responsible parties.

Statutory Debarment Activities within the Department

The OIG is conducting an audit of the Department's reporting and maintenance of statutory debarment actions. The audit objectives are to determine the extent that cases qualifying for statutory debarment are reported for inclusion in the Excluded Parties List System (EPLS) by the litigating components of the Department, the completeness and accuracy of records uploaded to the EPLS for statutory debarment actions maintained by the Department, and the timeliness of reporting statutory debarment actions to the EPLS.

Mortgage Fraud

The OIG is performing an audit of the Department's efforts to address mortgage fraud. Additionally, this audit will review component efforts to implement Department policy guidance, focusing on headquarters level programs and the coordination of components at the national level.

Ensuring Safe and Secure Non-Federal Detention Facilities

The OIG is conducting an audit of the Department's efforts to ensure a safe, secure, and humane environment for federal detainees held in non-federal detention facilities. This audit originally focused on the Office of the Federal Detention Trustee's efforts, but was expanded to recognize the role of other Department components, including the USMS.

Vetting Job Applicants

The OIG is reviewing the Department's process for checking the references of applicants being hired across a variety of job areas within both the excepted and competitive services.

Components' Security Clearances

The OIG review will examine whether the Department effectively manages the security clearance process for employees and contractors to meet component mission and security requirements. It will also assess if there are backlogs throughout the Department and the Department's success in meeting timeliness and reciprocity requirements of the *Intelligence Reform and Terrorism Prevention Act of 2004*.

Federal Bureau of Investigation

The FBI seeks to protect the United States against terrorist and foreign intelligence threats, enforces the criminal laws of the United States, and provides criminal justice services to federal, state, municipal, and international agencies and partners. FBI headquarters in Washington, D.C., coordinates activities of more than 35,500 employees in 56 field offices located in major cities throughout the United States and Puerto Rico, nearly 400 resident agencies in smaller cities and towns across the nation, and more than 60 international offices, called "legal attaches," in U.S. embassies worldwide.

Reports Issued

Progress in Responding to the Recommendations in the OIG's Report on the Fingerprint Misidentification in the Brandon Mayfield Case

The OIG issued a follow-up report examining the progress of the FBI in implementing the 18 recommendations contained in the OIG's March 2006 report, "A Review of the FBI's Handling of the Brandon Mayfield Case." Mayfield, an attorney in Portland, Oregon, was arrested by the FBI in May 2004 as a material witness after FBI Laboratory examiners identified Mayfield's fingerprint as matching a fingerprint found on a bag of detonators connected to the March 2004 terrorist attack on commuter trains in Madrid, Spain, that killed almost 200 people and injured more than 1,400 others. Mayfield was released two weeks later when the Spanish National Police identified an Algerian national as the source of the fingerprint on the bag. The FBI Laboratory subsequently withdrew its fingerprint identification of Mayfield.

The OIG's 2006 report on the Mayfield case concluded that the latent print examiners involved in the misidentification did not engage in intentional misconduct or violate any explicit FBI Laboratory procedures, but rather made errors in their application of the latent fingerprint methodology that reflected systemic problems with the FBI Laboratory's operations. In its follow-up review, the OIG found that the FBI Laboratory has made significant progress in implementing most of the OIG's original recommendations, including undertaking research to develop objective criteria for latent fingerprint analysis and substantially revising its standard operating procedures and training materials to address many of the causes of the Mayfield misidentification. Notable improvements include the following:

- Major revisions to the FBI Laboratory's standard operating procedures to provide specific standards for conducting latent fingerprint examinations and to require documentation of all phases of the process; and

- Substantial changes to the FBI Laboratory's procedures for verifying identifications to minimize bias and encourage a culture in which examiners feel free to disagree, and requiring

a mandatory blind verification for identifications based on a single latent fingerprint, like the one in the Mayfield case.

However, the follow-up review identified deficiencies with the monthly "Capital Case Review" that had been implemented in response to concerns identified following the Mayfield misidentification. At the time of the 2006 review, the FBI Laboratory and the Criminal Division were conducting the "Capital Case Review" of prisoners awaiting execution to determine whether the latent print unit had conducted analysis in the case that resulted in the death sentence, or in an earlier case that may have been an aggravating factor in the death penalty phase. The Criminal Division was periodically providing lists of prisoners scheduled for execution to the Laboratory, and the Laboratory was determining whether it had previously conducted fingerprint identifications in connection with the case. Although the review had identified no such cases as of March 2006, the OIG recommended in its 2006 report that the FBI Laboratory continue the Capital Case Review or adopt another procedure sufficient to accomplish the same objectives.

During the follow-up review, the OIG found that beginning in March 2008, the Criminal Division ceased providing names of prisoners scheduled for execution to the FBI Laboratory. The suspension of the Capital Case Review was not the result of a specific decision but rather an inadvertent consequence of personnel changes in the Criminal Division. At the urging of the OIG, the Criminal Division and the FBI Laboratory reinstated the Capital Case Review while the OIG was conducting its follow-up review.

Efforts to Combat National Security Cyber Threats

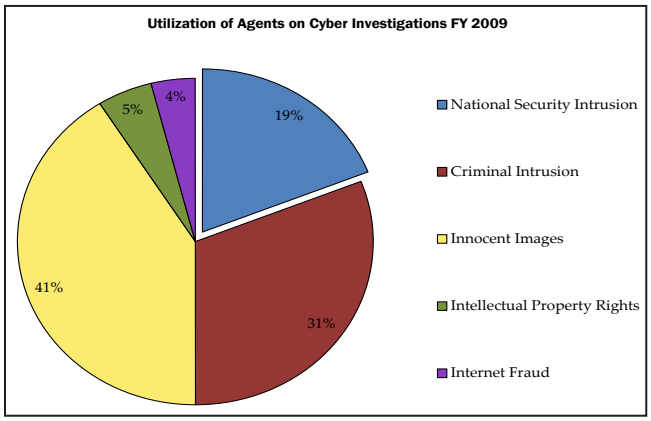
This OIG audit report focused on the FBI's efforts to develop the National Cyber Investigative Joint Task Force (NCIJTF) and the capabilities of FBI field offices to investigate national security cyber intrusion cases. Created by Presidential Directive, the NCIJTF is an FBI-led, multi-agency task force responsible for ensuring that the U.S. government coordinates its efforts to combat national security cyber intrusions. In 2008, the President established the Comprehensive National Cyber Initiative (CNC) to implement the responsibilities outlined in the Presidential Directive.

The audit found that the FBI has completed many of the interim goals for the NCIJTF developed under the CNC, which is intended to combine the missions of various federal agencies to defend against cyber intrusions. The FBI developed an operational plan for the NCIJTF, incorporated many intelligence community and law enforcement agencies in day-to-day NCIJTF operations, formed threat focus cells comprised of NCIJTF participants' with expertise in targeting specific cyber threats, and had some operational successes in mitigating cyber threats against the United States.

However, the OIG identified areas where the NCIJTF could improve its capabilities to defend against cyber attacks. Specifically, the NCIJTF did not always share relevant information about cyber threats among the task force's partner agencies. Further, the audit found that NCIJTF partner agencies had not agreed to a consistent information sharing framework as directed in the NCIJTF's operational plan. As a multi-agency task force, the OIG believes that it is vital that all NCIJTF partner agencies have a common understanding about what information will be shared.

In addition, the audit identified areas where the FBI could improve the capabilities of its

field offices to investigate national security cyber intrusion cases. For example, during the OIG interviews with 36 FBI agents assigned to investigate national security-related cyber intrusion cases at 10 FBI field offices, 13 of these agents (36 percent) reported not having the technical skill set that the FBI's Cyber Division officials had identified as necessary to investigate these types of cases. Moreover, 5 of the 36 agents (14 percent) advised that they did not believe they were able or qualified to investigate national security intrusions effectively.



Source: FBI

The audit found that the FBI's policy of rotating agents through different FBI field offices hindered the ability of some FBI field offices to investigate national security intrusions effectively. Because national security intrusion cases are highly technical and require a specific set of skills, new cyber agents are often not equipped to assume responsibility of a national security intrusion investigation. In 4 of the 10 offices visited, agents advised that they had been assigned cyber cases that exceeded their technical capabilities. Further, the audit found that some field agents believed field offices lacked adequate tactical analytical support for national security intrusion investigations, hampering their ability to "connect the dots" in an investigation and to determine those responsible for intrusions.

The report provided nine recommendations to help the FBI fully implement the NCIJTF and strengthen its cadre of field agents assigned to investigate national security cyber intrusions, and the FBI concurred with the recommendations.

Convicted Offender, Arrestee, and Detainee DNA Backlog

The OIG issued an audit report that determined that the FBI has effectively eliminated its backlog of DNA samples collected from federal convicted offenders, federal arrestees, and non-U.S. citizen detainees.

The FBI Laboratory analyzes and uploads convicted offender, arrestee, and detainee DNA samples into the Combined DNA Index System (CODIS) to identify matches with DNA profiles from unsolved cases or cases without a suspect, thereby providing investigative leads to law enforcement agencies. Historically, the FBI Laboratory has had a backlog of convicted offender, arrestee, and detainee samples, which was mainly the result of federal legislation enacted in the past 10 years that expanded the scope of DNA sample collection from violent federal convicted offenders to include anyone who commits a federal offense as well as non-U.S. citizens who are detained in the United States. In December 2009, the FBI Laboratory reported that it had a backlog of over 312,000 convicted offender, arrestee, and detainee DNA samples waiting to be processed.

The OIG determined that as of May 2011, the FBI had reduced its backlog to a workload of approximately 14,000 samples. Because the FBI currently has the capacity to analyze 60,000 DNA profiles per month and is able to begin processing accepted DNA samples within 30 days of receipt, we concluded that 14,000 samples was a manageable monthly workload and thus the backlog had been effectively eliminated.

The audit concluded that the FBI has achieved a significant accomplishment in reducing the convicted offender, arrestee, and detainee DNA backlog to a manageable monthly workload. The FBI achieved these results by implementing a backlog reduction strategy, hiring additional personnel and contractors, using high-throughput robotics, implementing software for a semi-automated review of DNA profiles after completion of analysis, and reconfiguring laboratory space for more efficient processing.

Comparison of Previous Methods of DNA Processing with Current Methods

Category of Comparison	Prior Method	One Robotic Line and Expert Software
Samples processed per day	510	1,700
Samples processed per month	8,000	30,000
Number of plates processed per day (1 plate = 85 Samples)	6	20
Sample Review	Manual review, 100 minutes per plate	Examiner assisted with Expert System software, 25 minutes per plate

Source: FBI presentation dated June 2009

While the FBI was successful in reducing its backlog, the audit identified some areas for improvement. The OIG found that the FBI Laboratory does not have documented policies, procedures, and reporting methods to ensure backlog and workload levels are accurately identified and reported to management. The lack of written policies and procedures can also cause inconsistent calculations and affect the ability to compare statistics over a period of time.

In addition, the OIG is concerned with the long-term storage of DNA samples. The FBI maintains its processed DNA samples indefinitely in the event that it might need to retest a sample to confirm a match. As of May 2011, the FBI Laboratory had over 712,000 DNA samples that required storage, and it anticipates having 1 million samples by the end of the calendar year. Currently, some samples are stored in the basement of the FBI Laboratory in boxes stacked from the floor to the ceiling. The FBI is in the process of procuring high density storage units and is considering long-term storage options, including off-site locations. However, these two initiatives are still in the planning stages.

The Federal DNA Database Unit Storage Space at the FBI Laboratory as of August 2011

Source: The Federal DNA Database Unit as of August 2011

Source: The Federal DNA Database Unit as of August 2011

The OIG made three recommendations to assist the FBI in more accurately identifying, reporting, and projecting its convicted offender,

arrestee, and detainee DNA sample workload, and to develop a long-term plan to store DNA samples, and the FBI agreed with the recommendations.

CODIS Audits

The FBI's CODIS is a national information repository that stores DNA specimen information to facilitate its exchange by federal, state, and local law enforcement agencies. During this reporting period, the OIG audited state and local laboratories that participate in CODIS to determine the laboratories' compliance with the FBI's Quality Assurance Standards and National DNA Index System (NDIS) participation requirements. Additionally, we evaluated whether the laboratories' DNA profiles in CODIS databases were complete, accurate, and allowable for inclusion in NDIS. Below are examples of our audit findings.

- The OIG audit of the Tucson, Arizona, Police Department Crime Laboratory (Laboratory) found that of 100 forensic profiles sampled, 93 were complete, accurate, and allowable for inclusion in NDIS. Of the remaining profiles, we determined that five profiles were unallowable because they could not be sufficiently connected to the crime, and the Laboratory deemed two other profiles inappropriate for upload to NDIS. The Laboratory removed all seven of the unallowable profiles from NDIS before we completed our fieldwork. As a result of the OIG's finding that the Laboratory retained personnel records for 5 years instead of the required 10 years, the FBI required the Laboratory to revise its personnel records retention policy to reflect NDIS participation requirements, and the Laboratory revised its manual accordingly. The OIG found the Laboratory to be in compliance with all other NDIS procedures we reviewed, including adequate Laboratory security, staff's awareness of NDIS procedures, completion of required annual training, and NDIS matches handled in accordance with requirements, as well as compliance with the Quality Assurance Standards we tested.

- The OIG audit found that the Tennessee Bureau of Investigation Memphis Regional Crime Laboratory (Laboratory) complied with the forensic Quality Assurance Standards we reviewed. However, the Laboratory was not storing a copy of the CODIS database backup at an offsite location on a monthly basis as required by NDIS participation requirements and did not provide documentation during the OIG's audit that it had responded to a request from another laboratory to confirm an NDIS match. The CODIS administrator obtained the documentation from the initiating laboratory after we completed the audit. Also, while the OIG was on site, the CODIS administrator removed from NDIS the four unallowable forensic profiles the OIG found out of the 100 sampled. The OIG made two recommendations to address the Laboratory's compliance with standards governing CODIS activities and the FBI agreed with the corrective actions taken by the Laboratory.

- In an audit of CODIS activities at the Texas Department of Public Safety Lubbock Criminal Laboratory (Laboratory), the OIG determined that CODIS access is properly safeguarded and the Laboratory is in compliance with Quality Assurance Standards tested. However, the audit noted that while NDIS requires personnel records be kept

for 10 years, the Laboratory's operations guide requires that personnel records be retained for only 5 years. The OIG recommended that the FBI ensure that the Laboratory amend its operations guide to reflect NDIS personnel records retention requirements, and the Laboratory agreed to work with the FBI to find a mutually agreeable solution regarding this policy. In addition, Laboratory officials took corrective action for the 2 forensic DNA profiles, out of 100 profiles sampled, that the OIG determined were unallowable for inclusion in the National DNA Index System.

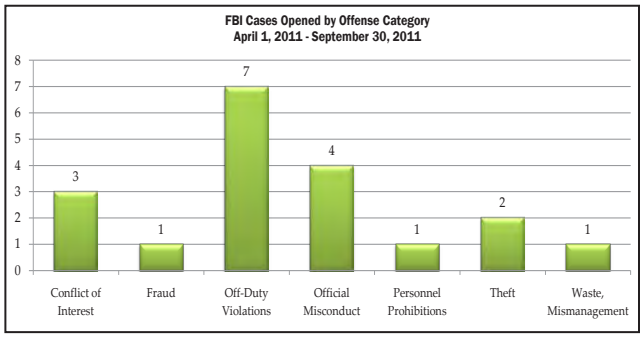
- The OIG audit at the Tarrant County Medical Examiner's Office Laboratory (Laboratory) in Tarrant County, Texas, found the Laboratory to be in compliance with the NDIS requirements and Quality Assurance Standards we tested. In addition, the Laboratory's 100 forensic DNA profiles that the OIG reviewed were complete and accurate. However, the Laboratory removed nine of these profiles from NDIS because they did not meet the NDIS requirements for inclusion. Because our findings were addressed before our final report was issued, our final audit report contained no recommendations.

- The OIG audit of the Texas Department of Public Safety McAllen Criminal Laboratory (Laboratory) in McAllen, Texas, found that, with the exception of the Laboratory's policy to retain personnel records for 5 years instead of the required 10 years, it was in compliance with the NDIS participation requirements and Quality Assurance Standards we tested. In addition, of the 100 forensic DNA profiles that we reviewed, 98 profiles were allowable for inclusion in NDIS. The Laboratory removed from NDIS two remaining profiles prior to our audit because, in one case, the Laboratory determined it was inappropriate, and in the other, it could not be determined if the profile was from the victim or the perpetrator.

Investigations

During this reporting period, the OIG received 812 complaints involving the FBI. The most common allegations made against FBI employees were official misconduct, waste and mismanagement, and off-duty violations. Most of the complaints received during this period were considered management issues and were provided to FBI management for its review and appropriate action.

During this reporting period, the OIG opened 19 investigations and referred 28 allegations to the FBI's Inspection Division for action or investigation. At the close of the reporting period, the OIG had 39 open criminal or administrative investigations of alleged misconduct related to FBI employees. The criminal investigations covered a wide range of offenses, including off-duty violations, official misconduct, and conflict of interest. The administrative investigations involved serious allegations of misconduct.



Source: Investigations Data Management System

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

- On August 10, 2011, an FBI Supervisory Senior Resident Agent was arrested and pled guilty on charges of making false statements. The Supervisory Senior Resident Agent admitted in pleading guilty that in 2010 he prepared a false evidence inventory and receipt form claiming that he had removed cash seized in a drug investigation in 2009 from FBI evidence and then placed it back into evidence at a local drug task force office. He admitted that he forged the signatures of two law enforcement officers as witnesses of the alleged transfer of cash on the evidence inventory and receipt form. The Supervisory Senior Resident Agent is no longer an FBI employee.

- On April 1, 2011, an FBI financial analyst assigned to the FBI Tampa Division in Tampa, Florida, was arrested and pled guilty to charges of theft of government property. In pleading guilty, the financial analyst admitted submitting fraudulent requests for disbursement of government funds through the FBI Tampa Division draft office. The financial analyst was sentenced in the Middle District of Florida to 60 months' probation and was ordered to pay $1,190 in restitution. The financial analyst retired from the FBI. The investigation was conducted by the OIG's Miami Field Office.

- In our September 2010 *Semiannual Report to Congress*, the OIG reported on an investigation that led to the arrest of an FBI Special Agent on charges of wire fraud, bank fraud, and bankruptcy fraud charges. The investigation by the OIG's Miami Field Office developed evidence that the Special Agent provided false information to obtain mortgage loans. In his mortgage applications, the Special Agent falsely claimed that he was employed by an alleged music company. The FBI Special Agent filed for bankruptcy in July 2009, and he failed to include properties the Special Agent owned or transferred on the bankruptcy application. During this reporting period, he was found guilty at trial on 15 counts of wire fraud and 3 counts of bankruptcy fraud and sentenced in the Middle District of Tennessee to 48 months' incarceration followed by 36 months' supervised release and was ordered by the court to pay $675,143 in restitution.

Ongoing Work

Integrity and Compliance Program

The OIG is reviewing how the FBI's Integrity and Compliance Program identifies risks of non-compliance with both the letter and spirit of applicable laws, regulations, rules, and policies; ranks identified risks; analyzes highly ranked risks; mitigates risks with adequate corrective actions; monitors the implementation of the corrective actions to ensure that mitigation is effective; and promotes a culture of integrity and ethical compliance throughout the FBI.

Management of Terrorist Watchlist Nominations and Encounters with Watchlisted Subjects

The OIG is continuing its audit of the FBI's management of terrorist watchlist nominations and encounters with watchlisted subjects. In FYs 2008 and 2009, the OIG conducted two audits related to the FBI terrorist watchlist nomination practices. In these audits, the OIG found that the FBI's procedures for processing international terrorist nominations were, at times, inconsistent and insufficient, causing watchlist data used by screening agencies to be incomplete and outdated. The OIG found that the FBI failed to nominate for watchlisting many subjects of its terrorism investigations, did not nominate many others in a timely manner, and did not update or remove watchlist records as required. As a result of these reviews, the FBI reported that it had undertaken several initiatives and implemented new processes and guidelines to enhance its watchlisting system.

The objectives of the OIG's ongoing audit are to assess the impact of recent events on the FBI's watchlisting system and evaluate the effectiveness of the initiatives recently implemented by the FBI to ensure the accuracy, timeliness, and completeness of the FBI's watchlisting practices, including watchlist nominations, modifications, and removals.

Activities Under Section 702 of the *FISA Amendments Act of 2008*

Section 702 of the *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008* (Act) authorizes targeting non-U.S. persons reasonably believed to be outside the United States to acquire foreign intelligence information. As required by the Act, the OIG is examining the number of disseminated FBI intelligence reports containing a reference to a U.S. person identity, the number of U.S. person identities subsequently disseminated in response to requests for identities not referred to by name or title in the original reporting, the number of targets later determined to be located in the United States, and whether communications of such targets were reviewed. In addition, the OIG is examining the FBI's compliance with the targeting and minimization procedures required under the Act.

Use of National Security Letters, Section 215 Orders, and Pen Register and Trap-and-Trace Authorities under *FISA* from 2007 through 2009

The OIG is again examining the FBI's use of national security letters (NSL) and Section 215 orders for business records. Among other issues, our review is assessing the FBI's progress in responding to the OIG's recommendations in prior OIG reports that examined the FBI's use of these authorities. Our review will also evaluate the automated system the FBI implemented to generate and track NSLs in response to the deficiencies identified in our prior reports, the number of NSLs issued and 215 applications filed by the FBI from 2007 through 2009, and any improper or illegal uses of these authorities. In addition, the review is examining the FBI's use of its pen register and trap-and-trace authority under the *Foreign Intelligence Surveillance Act of 1978* (FISA).

Aviation Operations

The OIG is conducting an audit to assess the management of FBI aviation operations and evaluate whether the use of official aircraft is appropriate and necessary to support official business operations. A similar but separate audit is being conducted of the DEA's management of aviation operations.

Sentinel

The OIG is continuing to evaluate the FBI's ongoing development and implementation of the Sentinel information technology project, which is intended to upgrade the FBI's electronic case management system and provide the FBI with an automated workflow process.

DNA Forensic Lab Backlog Follow-up

The OIG is conducting a follow-up audit of the FBI's forensic DNA case backlog. The audit will evaluate the status of the implementation of a laboratory information management system and progress towards a Department-wide laboratory information management system. It will also examine the effect of outsourcing agreements on the overall DNA forensic casework backlog, and assess any impending external factors that may impact the ability of the forensic DNA units to maintain their workload.

Follow-up Review Examining the FBI's Response to the Leung Report Recommendations

The OIG is conducting a follow-up review of the FBI's progress in implementing the recommendations contained in our May 2006 report, "A Review of the FBI's Handling and Oversight of FBI Asset Katrina Leung." The review is examining matters concerning the FBI's source validation process as well as FBI procedures governing agent interaction with sources.

Federal Bureau of Prisons

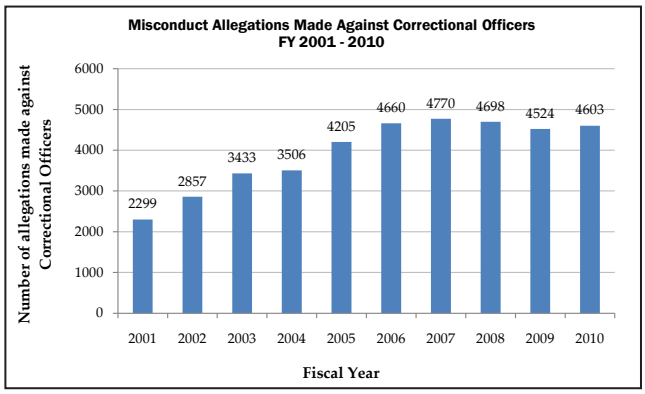
The BOP operates a nationwide system of prisons and detention facilities to incarcerate individuals imprisoned for federal crimes and detain those awaiting trial or sentencing in federal court. The BOP has approximately 38,000 employees and operates 116 institutions, 6 regional offices, and 2 staff training centers. The BOP is responsible for the custody and care of approximately 217,500 federal offenders, of whom more than 180,300 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.

Reports Issued

The BOP's Hiring Process

The OIG examined how the BOP screens correctional officers when making hiring determinations. The OIG conducted this review in response to the increase in correctional officer misconduct and arrests. The number of misconduct investigations opened by the BOP's Office of Internal Affairs against correctional officers doubled from FY 2001 to FY 2010, rising from 2,299 to 4,603 (see chart). During that same period, a total of 272 correctional officers were arrested, rising 89 percent from 18 in FY 2001 to 34 in FY 2010. Notably, 58 percent of the correctional officers who had substantiated allegations of misconduct and who received discipline of at least a 1-day suspension between FY 2001 and FY 2009 were disciplined for conduct that occurred within their first 2 years of service with the BOP.

The focus of the OIG's review was a statistical analysis of the relationship between the misconduct record of recently hired correctional officers and those officers' background characteristics, such as their record of discipline



Source: BOP Office of Internal Affairs data

at previous jobs, education level, and credit history. Although the BOP currently assesses such characteristics individually when deciding whether to hire or make a correctional officer a permanent member of the BOP's staff, the BOP does not conduct any systematic evaluation of combinations of background characteristics as part of its hiring process.

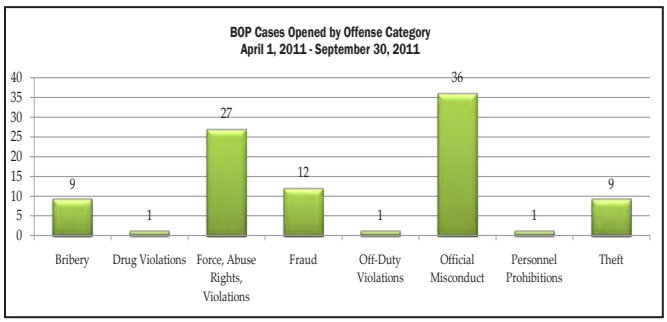
The OIG's analysis identified three combinations of background characteristics that have strong relationships with instances of substantiated misconduct resulting in at least a 1-day suspension during the first 2 years after a correctional officer begins work. The OIG's analysis further indicated that conducting an

evaluation of combinations of background characteristics in addition to individual characteristic evaluations could help the BOP reduce the likelihood of hiring correctional officers who will later commit misconduct. The OIG recommended that the BOP consider developing a composite scoring mechanism for assessing the suitability of correctional officer applicants, and the BOP agreed with the recommendation.

Investigations

During this reporting period, the OIG received 3,698 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 its review.

During this reporting period, the OIG opened 96 investigations and referred 18 allegations to the BOP's Office of Professional Responsibility (OPR) for action or investigation. At the close of the reporting period, the OIG had 181 open cases of alleged misconduct against BOP employees. The criminal investigations covered a wide range of allegations, including official misconduct and force, abuse, and rights violations.



Source: Investigations Data Management System

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

- On September, 1, 2011, a former BOP contractor and her husband were arrested and pled guilty to conspiracy to commit false statements relating to health care matters. The BOP contractor and her husband were operators of a company funded in part by Medicaid and which provided services to persons with developmental disabilities. In pleading guilty, the BOP contractor, who was a licensed psychologist working in the Education Department of a BOP facility in Texas, admitted that she obtained the personally identifiable information of inmates and used this information in a scheme to defraud Medicaid. In total, the BOP contractor and her husband fraudulently obtained $1,820,359 from the Texas Medicaid program. BOP had previously terminated the contract. The investigation was conducted by the OIG's Dallas Field Office and the Texas State Attorney General's Office, Medicaid Fraud Control Unit.

- A BOP correctional officer was arrested and pled guilty to charges of assaulting a federal inmate. In pleading guilty, the correctional officer admitted that the correctional officer assaulted an inmate. The BOP correctional officer was sentenced in the Eastern District of Tennessee to two years' probation. The BOP correctional officer is no longer employed by the BOP. The investigation was conducted by the OIG's Chicago Field Office.

- A BOP correctional officer was found guilty by a jury in the Middle District of Florida of sexual abuse of a ward. The evidence showed that the correctional officer engaged in sexual activity with a male inmate while she was on duty. The correctional officer had admitted to the OIG that she maintained a sexual relationship with the inmate and

resigned her position with the BOP. As part of her conviction, the correctional officer will be required to register as a sex offender. The investigation was conducted by the OIG's Miami Field Office.

- A BOP correctional officer was arrested and pled guilty to charges of bribery. The correctional officer provided tobacco and cell phones to inmates in exchange for money. The correctional officer admitted that he received approximately $30,000 to $40,000 in bribe payments in exchange for the contraband. He was sentenced in the Middle District of Florida to 37 months' incarceration followed by 24 months of supervised release and was fined $24,800. The correctional officer resigned his employment with the BOP. The investigation was conducted by the OIG's Miami Field Office and the DEA Tampa District Office.

- A BOP food services technician was arrested and pled guilty to charges of attempting to distribute and possess with the intent to distribute 100 grams or more of heroin. The food services technician admitted that he had smuggled contraband materials into the facility. The food services technician was sentenced in the Eastern District of North Carolina to 76 months' imprisonment followed by 4 years of supervised release.

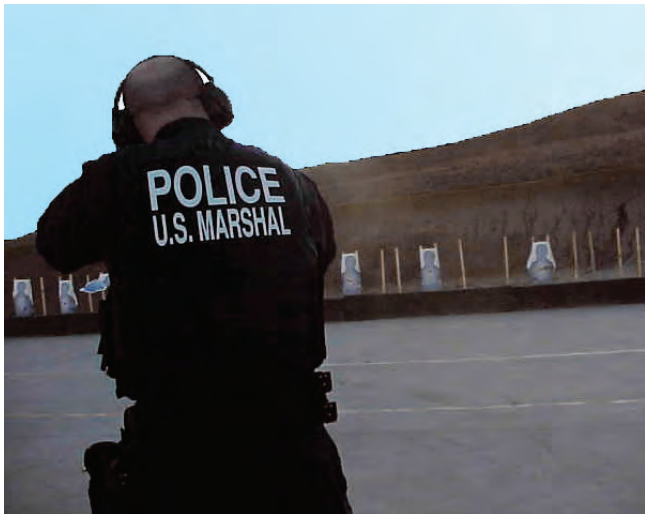
Ongoing Work

Residential Re-entry Centers Contracting and Management

The OIG is conducting an audit to evaluate the BOP's management of residential re-entry centers (RRCs). RRCs, also referred to as halfway houses, provide a structured, supervised environment as well as employment counseling, job placement, financial management assistance, and other programs and services to help inmates gradually rebuild their ties to the community. RRCs also facilitate supervising ex-offenders' activities during this readjustment phase. The audit objectives are to determine whether RRC operations are conducted in compliance with BOP requirements and if the BOP effectively administers and monitors its RRC contracts. The OIG is also reviewing whether the BOP administers its RRC contracts in accordance with applicable laws, regulations, and policies.

U.S. Marshals Service

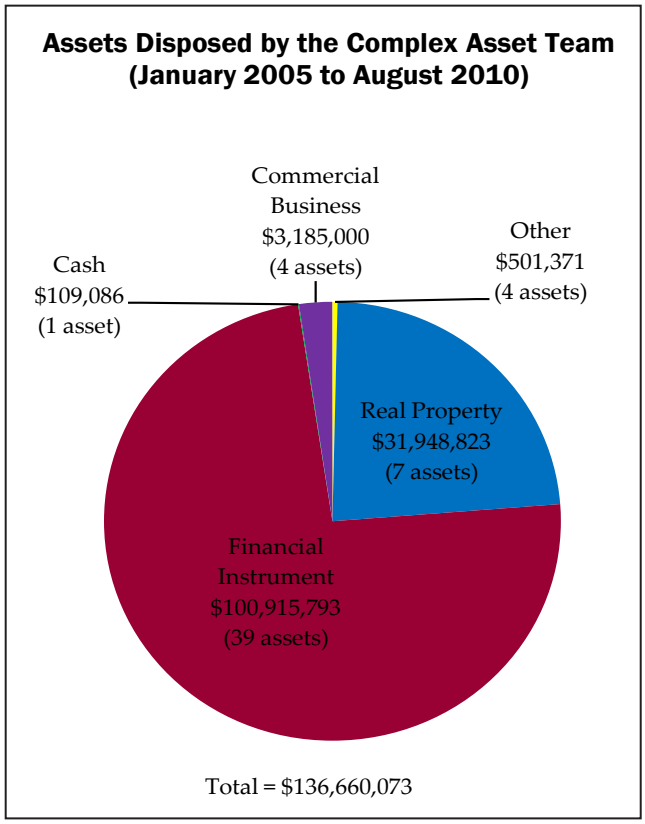
The USMS is responsible for ensuring the safe and secure conduct of judicial proceedings; protecting more than 2,000 federal judges and approximately 5,250 other court officials at more than 400 court facilities while providing security systems at nearly 900 facilities; arresting federal, state, and local fugitives; protecting federal witnesses; transporting federal prisoners; managing assets seized from criminal enterprises; and responding to major national events, terrorism, and significant high-threat trials. The USMS Director and Deputy Director work with 94 U.S. Marshals to direct approximately 5,675 employees at 316 locations throughout the 50 states, Guam, Northern Mariana Islands, Puerto Rico, U.S. Virgin Islands, Mexico, Jamaica, and the Dominican Republic.



Reports Issued

Administration of Complex Asset Team Management and Oversight

The OIG issued a report finding significant deficiencies in how the USMS managed complex assets, including those seized as part of financial crime cases, between 2005 and 2010. These deficiencies increased the Government's risk of mismanagement of the administration and disposition of forfeited assets. Since 2005, the Complex Asset Team — responsible for helping USMS district offices manage and dispose of unique and complicated assets that have been seized or forfeited to the federal government — has disposed of over $130 million in complex assets, including business and financial interests seized during investigations into several multi-million dollar financial crimes perpetrated by individuals including Ponzi-scheme operator Bernard Madoff, investment lawyer Scott Rothstein, banker and political fundraiser Hassan Nemazee, and organized crime figure James Galante.



Source: Records compiled by the USMS Complex Asset Team

The OIG found that the USMS did not have adequate procedures for managing, supervising, tracking, and keeping records on seized and forfeited complex assets. In the Bernard Madoff case, these inadequacies resulted in a loss of confidence in the USMS by prosecutors and others involved with the case. The audit found multiple instances in which a member of the Complex Asset Team valued and sold the same asset by himself, therefore having the final authority on many significant asset decisions with little or no oversight. Ultimately, the government hired external contractors to restart the disposition process for two Madoff assets, and all remaining Madoff assets administered by the Complex Asset Team were removed from the Team's responsibility.

In the Galante case involving organized crime, the USMS seized 25 waste disposal businesses that had outstanding tax liabilities unknown by the USMS at the time of seizure. These liabilities hindered the USMS's ability to sell the assets, which increased the time these assets were under seizure and in turn increased the risk that the assets would lose value.

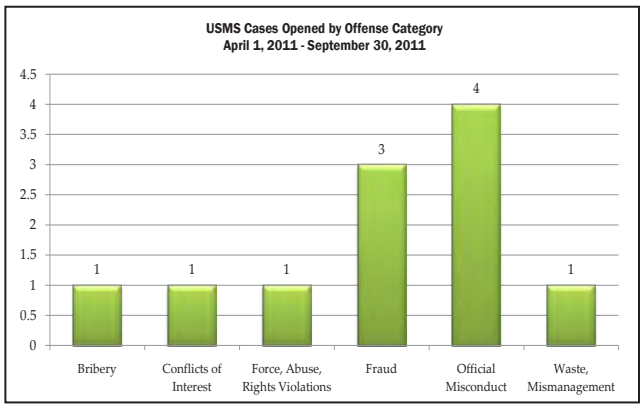
The OIG also found that the Complex Asset Team did not consistently document or conduct pre-seizure planning prior to seizing assets. The USMS's lack of planning exposed the government to unnecessary risk, such as seizing assets with significant liabilities or limited equity, or becoming involved in protracted litigation with third parties who have interests in the assets. In addition, inadequate tracking of assets administered led to discrepancies in the count between the USMS's physical records and its inventory of assets.

The report made 19 recommendations to help the USMS better manage and account for seized and forfeited complex assets. These recommendations included that the USMS should develop and implement formal procedures regarding the disposition of complex assets, ensure standardized and accurate recordkeeping procedures, conduct pre-seizure planning in collaboration with U.S. Attorneys' Offices and other investigative agencies, and bolster the legal, accounting and valuation knowledge of asset management staff. The USMS concurred with the recommendations and has begun to implement recordkeeping, reporting, and valuation procedural improvements. The report also made one recommendation to JMD to update the Consolidated Asset Tracking System so that local USMS district offices and the USMS Asset Forfeiture Division can use it to identify whether an asset is a complex asset that is being managed by the Complex Asset Team. JMD responded that it would coordinate with the USMS to implement this recommendation.

Investigations

During this reporting period, the OIG received 252 complaints involving the USMS. The most common allegations made against USMS employees included official misconduct, waste and mismanagement, off-duty violations, and force, abuse, and rights violations. The majority of the complaints were considered management issues and were provided to the USMS for its review and appropriate action.

During this reporting period, the OIG opened 11 investigations and referred 2 allegations to the USMS's Office of Internal Affairs for action or investigation. At the close of the reporting period, the OIG had 30 open cases of alleged misconduct against USMS employees.



Source: Investigations Data Management System

U.S. Marshals Service

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

- In our March 2011 *Semiannual Report to Congress*, the OIG reported on an investigation that led to the arrest and guilty plea of a former USMS administrative officer to theft of $104,000 in government funds. The former administrative officer admitted that she unlawfully used a USMS credit card for personal expenses, created a fictitious employee in the USMS payroll system and submitted falsified time and attendance records for the employee, facilitated the issuance of checks, and disguised the theft with fraudulent business invoices. Prior to this investigation, the former administrative officer had left the USMS in November 2008 and obtained employment with the DEA in a similar capacity. During this reporting period, the former USMS administrative officer was sentenced in the U.S. District Court for the District of Columbia, Washington, D.C., to 21 months' imprisonment followed by 36 months' supervised release and ordered to pay $104,000 in restitution.

- In our March 2011 *Semiannual Report to Congress*, the OIG reported on an investigation that lead to the arrest of a former Supervisory Deputy U.S. Marshal, previously assigned to the USMS Northern District of Illinois, Chicago Office, based on an indictment returned in the Northern District of Illinois charging him with making false statements to the OIG. The investigation by the OIG's Chicago Field Office determined that the Supervisory Deputy U.S. Marshal provided criminal history, motor vehicle, and driver license information obtained from restricted law enforcement databases to a friend who was under investigation by the FBI for staging fake accidents to collect insurance proceeds. The Supervisory Deputy U.S. Marshal provided false and misleading information regarding these actions during his OIG interview. During this reporting period, the Supervisory Deputy U.S. Marshal was sentenced to 36 months' probation and fined $5,000 pursuant to his guilty plea to charges of making false statements to the OIG. The Supervisory Deputy U.S. Marshal retired from the USMS.

Ongoing Work

Contract Management

The OIG is reviewing the USMS's policies and practices for awarding and administering contracts. The OIG seeks to determine whether the USMS complies with the Federal Acquisition Regulation, Department policies, and internal USMS policies in its award and administration of contracts; whether USMS internal controls ensure adequate contract oversight; and whether the USMS properly manages vendors to ensure contract requirements are met and contractor billings are accurate and complete.

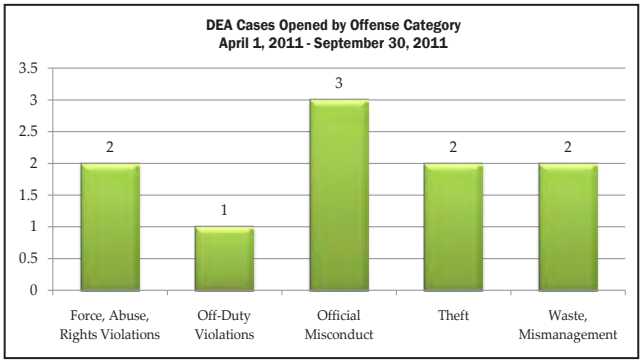
Drug Enforcement Administration

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 9,900 employees staffing its 21 division offices in the United States and 83 foreign offices in 63 countries.

Investigations

During this reporting period, the OIG received 311 complaints involving the DEA. The most common allegations made against DEA employees included official misconduct, waste and mismanagement, and theft. The majority of the complaints were considered management issues and were provided to the DEA for its review and appropriate action.

During this reporting period, the OIG opened 10 and referred 13 allegations to the DEA's OPR for action or investigation. At the close of the reporting period, the OIG had 15 open cases of alleged misconduct against DEA employees. The most common allegations were official misconduct; force, abuse, and rights violations; fraud; and theft.



Source: Investigations Data Management System

Ongoing Work

Adoptive Seizure Process

The OIG is examining the DEA's process for adopting seizures from state and local law enforcement agencies under the Department's Asset Forfeiture Program. State and local law enforcement agencies can seize property forfeited to them under state laws or they may transfer the property to a federal agency, such as the DEA, for forfeiture under federal laws. Seizures made by state and local law enforcement agencies that are accepted by a federal agency for processing under federal laws are known as "adoptive" seizures.

Aviation Operations

The OIG is conducting an audit of the DEA's management of aviation operations. The audit will assess the management of DEA aviation operations and evaluate whether the use of official aircraft is appropriate and necessary to support official business operations. A similar but separate audit is being conducted of the FBI's management of aviation operations.

Drug Enforcement Administration

Resource Management

In addition to examining how the DEA allocates and assesses personnel resources within its established priorities, the OIG is examining the allocation and utilization of DEA personnel on narcotics-related investigations and the number and types of drug investigations handled by the DEA.

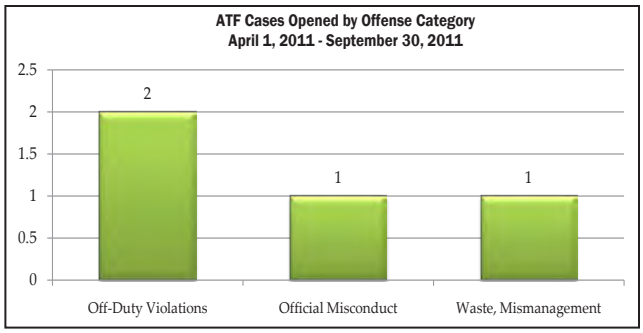
Bureau of Alcohol, Tobacco, Firearms and Explosives

ATF's 5,100 employees enforce federal criminal laws and regulate the firearms and explosives industries. ATF investigates violent crimes 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 25 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 Iraq, as well as a Regional Firearms Advisor based in San Salvador serving El Salvador, Guatemala, Nicaragua, Panama, Belize, Honduras, and Costa Rica.

Investigations

During this reporting period, the OIG received 285 complaints involving ATF personnel. The most common allegations made against ATF employees were waste and mismanagement and official misconduct. The majority of the complaints were considered management issues and were provided to ATF for its review and appropriate action.

During this reporting period, the OIG opened four cases and referred seven allegations to ATF's OPR for action or investigation. At the close of the reporting period, the OIG had 11 open criminal or administrative investigations of alleged misconduct related to ATF employees. The criminal investigations include off-duty violations.



Source: Investigations Data Management System

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

- On April 11, 2011, an ATF Special Agent assigned to the Washington Field Division pled guilty to charges of theft of public property, possessing or receiving stolen firearms, false statements, wire fraud, and money laundering. In pleading guilty, the Special Agent admitted that in his official capacity, he converted ATF seizures of firearms, tobacco, and currency to his personal use. Also, the Special Agent

admitted that he falsified official ATF documents relating to the disposition of the firearms and made unauthorized sales of tobacco product inventory and retained the proceeds. The Special Agent was subsequently sentenced in the Eastern District of Virginia to 37 months' imprisonment followed by 2 years of supervised release and ordered to pay $10,210 in restitution as well as forfeiture of $4,860 in recovered government funds. The Special Agent resigned from ATF. The investigation by the OIG's Washington Field Office was conducted with the assistance of ATF and the City of Hampton, Virginia, Police Department.

Ongoing Work

Federal Firearms Licensee Inspection Program

The OIG is reviewing ATF's federal firearms licensee inspection program. After an OIG review in 2004, ATF made a series of changes to that program and its administrative action process. This review is assessing the changes made to the program, ATF's process for inspecting licensed firearms dealers, the process for referring suspected criminal violations, and how ATF institutes administrative actions on licensed dealers that violate federal firearms laws and regulations.

Explosives Industry Program

The OIG is reviewing whether ATF's Explosives Industry Program complies with the *Safe Explosives Act* requirement to inspect all explosives license and permit holders at least once every 3 years and whether ATF analyzes information the program gathers to improve the program.

Income-Generating Undercover Operations

The OIG is conducting an audit of ATF's income-generating undercover operations to assess ATF's management of the revenue generated from these operations and its management of funds appropriated for the program. The OIG also seeks to determine whether ATF ensures that proceeds from income-generating undercover operations are properly allocated at the conclusion of the operations.

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 levels. OJP is composed of 5 bureaus – Bureau of Justice Assistance (BJA), Bureau of Justice Statistics (BJS), 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 and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. In this section, we discuss OJP's oversight of grant funds awarded through the regular appropriations process. We discuss our work related to OJP's oversight of grant funds awarded under the *American Recovery and Reinvestment Act of 2009* in a separate section in this semiannual report.

Reports Issued

Audits of Grants to State and Local Entities

The OIG conducts audit of various grants and other financial assistance provided by OJP to recipients outside of the Department. These recipients include state and local governments, universities, non-profit agencies, and for-profit agencies. During this reporting period, the OIG conducted four audits of external OJP recipients.

- The OIG audited two awards totaling $1,250,000 to Enough is Enough in Reston, Virginia, which creates educational programming to raise public awareness about the dangers of internet pornography and sexual predators, such as its *Internet Safety 101* program that provided training to protect children from online threats. The audit found that Enough is Enough did not follow standard accounting practices and did not maintain adequate internal controls to ensure compliance with grant requirements. The audit questioned over $800,000 in unsupported or unallowable costs for reasons such as missing documentation, authorizations, vouchers, receipts, or invoices as well as drawdowns in excess of general ledger expenditures and unapproved budget transfers. The OIG recommended that OJJDP require that Enough is Enough remedy questioned costs and implement internal controls. OJJDP agreed with our recommendations and responded that it will coordinate with Enough is Enough to remedy all questioned costs and address internal control deficiencies.

- The OIG audited the cooperative agreement awarded to Occupational Research and Assessment, Incorporated

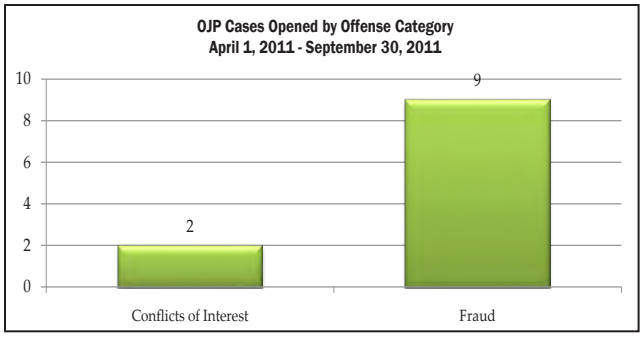
(ORA), in Big Rapids, Michigan, for $898,349 for a forensic science training development and delivery program for stakeholders involved with the National Missing and Unidentified Persons System. The audit found that while ORA was accomplishing or making adequate progress in meeting the grant objectives, some internal accounting weaknesses and reporting deficiencies existed. As a result, the audit questioned $138,310 in unsupported expenditures and recommended that OJP work with ORA to remedy these costs, improve accounting and internal control procedures, and correct reporting deficiencies. OJP agreed with the recommendations and is coordinating with ORA to implement appropriate corrective action.

- The OIG audited two grants totaling $5,057,900 awarded to the University of North Texas Health Science Center (UNTHSC) under the Using DNA Technology to Identify the Missing project. The University of North Texas Center for Human Identification, which is housed at the UNTHSC, receives federal funding to analyze DNA samples from both unidentified remains as well as reference samples from family members of missing persons. The audit could not verify the accuracy of the data included in the UNTHSC's progress reports for lack of supporting documentation and questioned over $130,000 in costs due to unallowable salary expenses, an employee whose salary did not comply with a special condition, and unauthorized time charged to the grant. OJP agreed with the audit's four recommendations and indicated it would coordinate with UNTHSC to remedy questioned costs, address the unallowable salary expenses and unauthorized time charged to the grant, and ensure that proper source documentation is maintained.
- The OIG audited a $1,124,000 award to the Best Friends Foundation (Best Friends), which operates several educational programs in the Washington, D.C., metropolitan area, and found that Best Friends did not maintain adequate internal controls to ensure compliance with grant requirements. Thus, internal control issues limited the OIG's ability to reconcile financial status reports and drawdown requests to Best Friends' accounting records. The audit also identified $182,881 in costs inappropriately charged to the grant. The OIG made 13 recommendations to OJP to work with Best Friends to remedy these costs and implement written policies to correct inadequate internal controls. OJP agreed with all 13 recommendations and indicated that it is working with Best Friends to remedy questioned costs and ensure it develops and implements strong accounting procedures.

Investigations

During this reporting period, the OIG received 30 complaints involving OJP. The most common allegation made against OJP employees, contractors, or grantees was fraud.

During this reporting period, the OIG opened 11 cases. At the close of the reporting period, the OIG had 26 open criminal or administrative investigations of alleged misconduct related to OJP employees, contractors, or grantees. The majority of these criminal investigations were related to fraud.



Source: Investigations Data Management System

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

- On August 29, 2011, a retired naval officer was found guilty by a jury in the U.S. District Court for the District of Columbia for filing a false claim with the September 11th Victim Compensation Fund and stealing approximately $151,000 from the government. The evidence at trial showed that the retired naval officer was stationed at the Pentagon on September 11, 2001, and claimed that he was injured during the terrorist attack on the building. He claimed the injuries that he suffered prevented him from playing competitive lacrosse and doing home improvement work. The evidence showed that the retired naval officer continued to play competitive lacrosse, ran the New York City Marathon in November 2001, and falsified documents submitted to the Victim Compensation Fund. The investigation was conducted by the OIG's Fraud Detection Office.

- On September 12, 2011, the U.S. District Court for the Southern District of New York ordered Mario Mastellone to pay a civil judgment of $3,241,367 for violating the *False Claims Act*. Following the September 11, 2001, terrorist attacks on New York, Mastellone submitted an application to the Department of Justice September 11th Victim Compensation Fund. In his application, he claimed that he was totally and permanently disabled in connection with the terrorist attacks. In June 2008, following a joint investigation by the OIG's Fraud Detection Office and the New York Field Office, Mastellone pled guilty to stealing $1,076,789 from the fund and was sentenced to 30 months' incarceration followed by 3 years of supervised release. The civil judgment against Mastellone ordered him to pay triple the amount stolen from the government.

Ongoing Work

OJJDP Award to the National Council on Crime and Delinquency

The OIG has initiated an audit of an OJP award made to the National Council on Crime and Delinquency (NCCD) to support Office of Juvenile Justice and Delinquency Prevention research. Specifically, the award provides funding for NCCD's project, Evaluating the Effectiveness of the Juvenile Detention Alternatives Initiative to Decrease Disproportionate Minority Contact and Detention of Status Offenders. The audit objectives are to determine whether the award was made fairly and appropriately, and determine whether NCCD has any actual or potential conflicts of interest that may adversely affect its performance under the award.

Civil Division

Investigations

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

- In the September 2009 *Semiannual Report to Congress* the OIG reported on a joint investigation by the OIG's Washington Field Office and the DEA that resulted in the arrest of a Civil Division legal secretary assigned to the Commercial Litigation Section on charges of conspiracy to distribute cocaine and possession with intent to distribute cocaine. During this reporting period, the legal secretary was found guilty by a jury for conspiracy to distribute cocaine, attempted possession with intent to distribute cocaine, possession with intent to distribute cocaine, and possession of a firearm in furtherance of a drug offense. He was sentenced to 248 months' incarceration, followed by 5 years of supervised release, and ordered to forfeit $100,000 in proceeds of the drug conspiracy.

Civil Rights Division

Ongoing Work

Enforcement of Civil Rights Laws by the Voting Section

The OIG is reviewing the enforcement of civil rights laws by the Voting Section of the Department's Civil Rights Division. The review is examining the types of cases brought by the Voting Section and any changes in the types of cases over time; any changes in Voting Section enforcement policies or procedures over time; whether the Voting Section has enforced the civil rights laws in a non-discriminatory manner; and whether any Voting Section employees have been harassed for participating in the investigation or prosecution of particular matters.

Office of Community Oriented Policing Services

Reports Issued

Audits of COPS Grants

COPS awards grants to state, local, territory, and tribal law enforcement agencies to hire and train community policing professionals, acquire and deploy crime-fighting technologies, and develop and test policing strategies. During this reporting period, we audited four external COPS grants recipients. The results of those audits are summarized below:

- The OIG audited a $607,945 Technology Program Grant awarded to the Corcoran Police Department (Corcoran) in Kings County, California, from funds earmarked in the *2008 Consolidated Appropriations Act* to fund "law enforcement technologies and interoperable communications program." Corcoran requested funding and subsequently received the COPS technology grant award to pay the salaries and fringe benefits for four police officers that would be re-assigned to work on the Kings County Narcotics Task Force. As of February 2011, $599,523 (99 percent) of grant funds were spent on the salaries and fringe benefits of the four officers, the purchase of one radio, and some ammunition. The OIG believes that COPS did not act in accordance with the *2008 Consolidated Appropriations Act* when it awarded technology funds to pay for police officer salaries and fringe benefits. Because COPS approved grant funds for a use not encompassed by the statute authorizing the program, the OIG recommended that COPS establish a process to ensure that it approves only grant applications that comply with related funding legislation. Based on the findings relating to Corcoran and its sub-recipients, we questioned $321,829 and made 12 additional recommendations for COPS to ensure that Corcoran strengthen its internal controls. COPS agreed with our recommendations.

- The OIG audited nearly $3.5 million in COPS Technology Program grants awarded from 2005 to 2009 to the City of Albuquerque, New Mexico (City), to upgrade communications and computer equipment for the Albuquerque Police Department's Comprehensive Information Systems Project. All of the grants were earmarks, awarded through Congressional appropriations, and without regard to unresolved OIG audit findings. At the time of our audit, the City was considered high risk and barred from receiving COPS grants from September 2010 to September 2014 due to supplanting. The OIG identified instances of poor accounting practices, identified $99,423 in questioned costs and indications of supplanting in wages and fringe benefits, and made 11 recommendations for COPS to ensure that the City implement appropriate procedures, controls, and policies to fulfill grant requirements and remedy questioned costs. COPS concurred with our recommendations and is working with the City to implement the recommendations.

- The OIG audited a $746,934 Technology Program Grant awarded to the Township of Kalamazoo, Michigan, to assist with the purchase and installation of a radio

tower to enhance communications in areas that have poor, or in some cases, no radio coverage. The OIG found minor instances of noncompliance with regard to COPS grant requirements, including that Kalamazoo Township lacked a policy to regularly change passwords for its automated accounting system; its 2008 and 2009 progress reports were filed 19 and 3 days late, respectively; its property records did not identify as federally funded equipment that was purchased with federal funds; and it lacks a formalized policy for accountable property. The OIG made four recommendations, which COPS agreed with and which the grantee has taken steps to implement.

- The OIG audited a $250,000 Technology Program Grant awarded to the Sherwood Police Department (Sherwood) in Sherwood, Oregon, for the purpose of establishing a local interoperable wireless communications network. Overall, the audit found that Sherwood adequately maintained grant-related financial records and properly managed the use of grant funds. However, the OIG found that Sherwood's Delegation of Contracting Authority was outdated and that Sherwood lacked a comprehensive implementation plan for how it planned to complete the installation of the interoperable wireless communications network before the grant expired. The OIG made two recommendations. COPS and Sherwood concurred with the OIG's recommendations and are taking appropriate actions to implement the recommendations.

Investigations

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

- On July 28, 2011, Zachary Hannan and his company Prime Distribution LLC were issued formal suspension notices from the Senior Procurement Executive at JMD and proposed for debarment from contracting with any federal agency and from receiving any federal grants. Hannan previously pled guilty to charges of misapplication of federal grant funds and making false statements and was sentenced in the Southern District of Illinois to 12 months plus one day of incarceration. Hannan reimbursed the county $71,333 for the missing grant funds prior to his indictment. The investigation of this matter was conducted by the OIG's Chicago Field Office and the FBI.

Criminal Division

Reports Issued

Equitable Sharing Audits

Under the Department's Asset 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. Equitable sharing revenues represent a share of the proceeds from the forfeiture of assets seized in the course of certain criminal investigations.

During this reporting period, the OIG examined equitable sharing revenues received by four law enforcement agencies. The results of two of these audits follow:

- The Department of Police of Montgomery County, Maryland (MCPD), received over $270,000 during the 2-year period beginning July 2008

and ending June 2010 as a participant in the Department's equitable sharing program. The OIG found that the MCPD did not adequately account for or track $27,998 received in FY 2010 and understated its expenditures in its FY 2010 Agreement and Certification Form by approximately $36,800. The audit identified $20,199 in questioned costs that were unallowable under Department equitable sharing guidelines. The OIG made five recommendations for the Criminal Division to ensure that MCPD correct weaknesses in its procedures and remedy questioned costs. The MCPD and the Criminal Division agreed with the OIG's recommendations.

- The Police Department of Cleveland, Ohio (Cleveland PD), received $256,496 in equitable sharing revenues for calendar year 2009 to support law enforcement operations. While the OIG found that the Cleveland PD generally complied with equitable sharing guidelines, the audit identified expenditures for college courses not specifically related to law enforcement, and as a result, the audit reported $5,971 in questioned costs. In addition, the audit found that the Cleveland PD did not accurately report all interest income and commingled some of its Department equitable sharing funds with equitable sharing funds from the Treasury. The OIG recommended that the Criminal Division ensure that the Cleveland PD file accurate and timely reports and separately account for Department and Treasury equitable sharing funds. The Criminal Division agreed with our recommendations, is working with the Cleveland PD to improve its procedures, and has requested that the Cleveland PD refund $5,971 to its equitable sharing account.

Ongoing Work

Office of Overseas Prosecutorial Development, Assistance, and Training and the International Criminal Investigative Training Assistance Program

The Criminal Division's Office of Overseas Prosecutorial Development, Assistance, and Training (OPDAT), and the International Criminal Investigative Training Assistance Program (ICITAP) provide training and technical assistance to foreign countries' prosecutors, judicial personnel, and law enforcement personnel. The OIG is reviewing the programs' controls and practices related to funding, security, travel, and reimbursable agreements, as well as the programs' coordination with other U.S. agencies and foreign components.

Environment and Natural Resources Division

Reports Issued

Superfund Activities for FYs 2009 through 2010

The OIG's Audit Division examined the Department's Superfund activities in the Environment and Natural Resources Division (ENRD) for FY 2009 through FY 2010. The *Comprehensive Environmental Response, Compensation and Liability Act of 1980* (known as CERCLA or Superfund), which was expanded by the *Superfund Amendments and Reauthorization Act of 1986*, established the Superfund program

to clean up the nation's worst hazardous waste sites. The OIG conducted this audit to determine if the cost allocation process used by ENRD and its contractor provided an equitable distribution of total labor costs, other direct costs, and indirect costs to Superfund cases during FY 2009 through FY 2010.

Based on the results of the audit, the OIG concluded that ENRD provided an equitable distribution of total labor costs, other direct costs, and indirect costs to Superfund cases. However, during the comparison of costs reported by the contractor and those recorded in the Department's accounting records, the OIG found that ENRD did not maintain copies of all data it provided to the contractor, including initial financial data, and correspondence and reconciliations made between ENRD and the contractor.

The OIG recommended that ENRD develop processes to maintain documentation in order to provide complete support for the Superfund allocation processes and aid in the reconciliation of ENRD and contractor data. ENRD agreed with the recommendations.

Executive Office for Immigration Review

Ongoing Work

Administration of Immigration Courts

The OIG is examining the Executive Office for Immigration Review's (EOIR) efforts to manage the pending caseload in its immigration courts. This includes analyzing characteristics of the caseload, such as case types and case ages, along with evaluating case processing methodology. The OIG will also report on EOIR's implementation of reform measures designed to improve the performance of immigration judges and the Board of Immigration Appeals.

U.S. Attorneys' Offices

Investigations

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

- An investigation by the OIG's Dallas Field Office determined that a legal assistant assigned to a USAO made unauthorized disclosures of law enforcement sensitive information. The legal assistant resigned her employment from the USAO.

Office on Violence Against Women

Reports Issued

Audits of OVW Grants

The OVW administers financial and technical assistance to communities across the country for the development of programs, policies, and practices aimed at ending domestic violence, dating violence, sexual assault, and stalking. OVW recipients include state and local governments, universities, non-profit agencies, and for-profit agencies. The following audit was conducted during this reporting period:

- The OIG audited over $1.3 million in OVW grants to Jane Doe, Inc., also known as the Massachusetts Coalition Against Sexual Assault and Domestic Violence. The awards covered four

grants for victim services, training for law enforcement, programs for victim advocates, and creating jobs. The audit identified numerous internal control weaknesses, including unsupported and unallowable payroll expenditures, unallowable bonus payments, and unallowable and unreasonable conference expenditures. In addition, a contractor performing grant funded services was not effectively monitored and Jane Doe did not comply with all of the grants' special conditions. Because of these deficiencies, the OIG questioned $638,298, or about 47 percent, of the grant funds and made 11 recommendations to improve the grantee's internal controls and remedy questioned costs. OVW agreed with the recommendations and is working with Jane Doe, Inc., to implement the recommendations.

Investigations

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

- The former executive director of a Department grantee was arrested pursuant to an indictment charging her with theft from a program receiving federal funds. The indictment alleged that between May 31, 2005, and August 5, 2010, the former executive director received 36 payroll advances and failed to pay back $12,960.98, and that the former executive director converted Department grant funds for travel-related expenses for herself or her friends and family. This investigation was conducted by the OIG's Denver Field Office.

American Recovery and Reinvestment Act of 2009

The *American Recovery and Reinvestment Act of 2009* (Recovery Act) provides $787 billion in funding as a stimulus to the economy. Of that funding, the Department received $4 billion for grant funding to enhance state, local, and tribal law enforcement; to combat violence against women; and to fight Internet crimes against children.

The OIG is conducting aggressive Recovery Act oversight involving the coordinated efforts of auditors, investigators, and inspectors. Through this multidisciplinary effort, the OIG has provided advice to Department granting agencies regarding best practices in the awarding and monitoring of grants, trained Department grant managers on fraud risks, reached out to state and local agency Recovery Act recipients of Department grant funds, audited and evaluated the Department's use of Recovery Act funding, and conducted investigations of allegations of misuse of Recovery Act funds by Department grant recipients.

In particular, since the enactment of the Recovery Act in February 2009, the OIG has trained 5,838 federal, state, and local program managers and participants on Recovery Act fraud awareness, conducted 106 outreach sessions with state and local agencies, and initiated 41 audits and reviews of Recovery Act funds. In addition, the OIG is conducting nine investigations of allegations pertaining to the Department's Recovery Act programs. During this semiannual reporting period, the OIG issued four reports on the Recovery Act grant management activities of the Department as well as state and local entities.

From enactment of the Recovery Act in February 2009 through September 30, 2011, the Department has obligated more than 99 percent of its $4 billion in Recovery Act funds. Moreover, as of September 30, 2011, the Department had expended about 72 percent of its Recovery Act funds. The Department has handled this increased workload without any significant increase in staff.

We provide a summary below of our findings from our audit work during this review period that related to Recovery Act funds.

Reports Issued

OIG Audits of Recovery Act Grants

During this reporting period, the OIG audited Recovery Act grants awarded by Department grant-awarding agencies to state and local recipients. Below are examples of our audit findings:

- The OIG audited $1,246,494 in Recovery Act and non-Recovery Act grants awarded to the City of Suisun City, California (Suisun City), to fund criminal justice operations in both county and city jurisdictions. The audit found that Suisun City generally complied with essential grant requirements but that some expenditure information reported to the awarding agency did not match Suisun City's official accounting records. In addition, even though the grants were technically for 4 years, one sub-recipient had yet to purchase and install security cameras that were funded by both the Recovery Act and

non-Recovery Act grants. The OIG made two recommendations to ensure consistent reporting and accomplish grant objectives. OJP agreed with both recommendations.

- The OIG audited over $5 million in Edward Byrne Memorial Justice Assistance Grants, including a Recovery Act grant, awarded to the City of Birmingham, Alabama (Birmingham). The audit identified several deficiencies regarding compliance with the grants' requirements, including that City of Birmingham did not maintain adequate property records indicating the source of the funds used to acquire the items; did not provide sufficient information in grant progress reports; could not show that it had met grant goals and objectives; and did not monitor and had no procedures for monitoring sub-recipients. The audit identified $2,513 in unallowable costs and found that $55,825 in grant funds were spent on property items that were being kept in storage until needed by the police department. The OIG made eight recommendations to OJP to ensure that Birmingham implements appropriate processes and procedures to satisfy grant requirements, including an adequate property records system, detailed progress reports, and identifying and tracking measurable goals for each grant. OJP agreed with our recommendations.

- During this reporting period, the OIG audited an $837,721 Recovery Act Rural Law Enforcement Assistance grant awarded to the City of Aberdeen, Washington (Aberdeen). Aberdeen used the grant to retain four corrections officers and hire two new corrections officers for 2 years to continue operations at its 18-bed jail facility during the economic downturn. The OIG found that Aberdeen made a reasonable effort to accomplish grant objectives. However, the audit found that Aberdeen comingled grant-related payroll expenditures with non-grant related transactions, and questioned $9,563 of some corrections officer salaries that were not adequately supported with properly approved timecards. The OIG made four recommendations to OJP to help ensure that Aberdeen adhere to grant requirements, including submitting accurate financial reports. OJP agreed with our recommendations and indicated it would coordinate with Aberdeen to remedy questioned costs and ensure compliance.

Investigations

- On August 23, 2011, the mayor of Kinloch, Missouri, Keith Conway, was arrested and pled guilty to charges of wire fraud and theft of funds from a federal program. Kinloch received $90,000 in Recovery Act funds from a COPS grant. In entering his guilty plea, the mayor admitted that he used city funds to pay for several luxury items.

- On September 27, 2011, an individual was arrested on federal charges of theft of government property and bank fraud. The investigation by the OIG's Atlanta Area Office resulted in charges that the individual allegedly used a stolen identity and fraudulent documents to open a bank account to deposit a stolen check. The check was issued by OJP pursuant to a grant of funds from the Recovery Act.

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 OIG's top challenges for the year are listed here. Many of the challenges remain on the list from last year — "Counterterrorism," "Restoring Confidence in the Department," "Southwest Border Security Issues," "Protecting Civil Rights and Civil Liberties," "Information Technology Systems Planning, Implementation, and Security," and "Detention and Incarceration," in recognition of the long standing nature of these challenges.

The challenge of "Implementing Cost Savings and Efficiencies" was added to recognize the difficult challenges the Department faces in continuing to implement its mission in this constrained fiscal climate.

In addition, we have re-categorized two of last year's challenges so that the issues previously represented by "Violent and Organized Crime" and "Financial Crimes and Cyber Crimes" are represented in this year's list as "Criminal Law Enforcement" and "Financial Enforcement" in order to recognize the Department's efforts beyond criminal law enforcement. "Financial Enforcement" includes matters such as mortgage fraud, *False Claims Act* litigation and recoveries, civil penalty enforcement, asset forfeiture, and suspension and debarment. "Criminal Law Enforcement" includes elements of violent and organized crime as well as cyber crime and international crime.

Also, last year's "Grant Management" challenge has been expanded and renamed "Grants and Contract Management." In addition to grant management, it will also focus on how the Department handles procurement and acquisition issues.

Top Management and Performance Challenges in the Department of Justice – 2011

1. Counterterrorism
2. Implementing Cost Savings and Efficiencies
3. Southwest Border Security Issues
4. Protecting Civil Rights and Civil Liberties
5. Information Technology Systems Planning, Implementation, and Security
6. Criminal Law Enforcement
7. Restoring Confidence in the Department
8. Financial Enforcement
9. Detention and Incarceration
10. Grants and Contract Management

Detailed information about the Department's management and performance challenges can be found online at www.justice.gov/oig/challenges/.

Congressional Testimony

During this reporting period, the Acting Inspector General testified before the U.S. House of Representatives Committee on Oversight and Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and Procurement Reform, regarding the Department's oversight of grants programs.

Legislation and Regulations

The *Inspector General 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 could affect its operations and legislation that relates to waste, fraud, or abuse in the Department's programs and operations.

During the reporting period, the OIG reviewed and provided comments on a variety of proposed legislation and regulations, including the proposed legislation entitled *Digital Accountability and Transparency Act*.

Statistical Information

Audit Overview

The OIG's Audit Division issued 52 internal and external audit reports, which contained more than $2.5 million in questioned costs and made 225 recommendations for management improvement. Specifically, the Audit Division issued 25 internal audit reports of Department programs and 27 external audit reports of contracts, grants, and other agreements funded at over $34 million; and 14 *Single Audit Act* audits of programs funded at more than $12 million. In addition, the Audit Division issued two Notifications of Irregularities.

Questioned Costs			
Reports	**Number of Reports**	**Total Questioned Costs (including unsupported costs)**	**Unsupported Costs**
Audits			
No management decision made by beginning of period[1]	12	$7,325,302	$116,781
Issued during period	18[2]	$2,750,206	$1,968,909
Needing management decision during period	30	$10,075,508	$2,085,690
Management decisions made during period: -Amount of disallowed costs[3] -Amount of costs not disallowed	26 2	$4,353,847 $5,696,286	$2,080,514 $0
No management decision at end of period	2	$25,375	$5,176
Evaluations			
Nothing to report from the Evaluation and Inspections Division.			
Special Reviews			
Nothing to report from the Oversight and Review Division.			

1 Reports previously issued for which no management decision has been made.
2 Of the audit reports issued during this period with questioned costs, three were *Single Audit Act* reports.
3 Includes instances in which management has taken action to resolve the issue and/or the matter is being closed because remedial action was taken.

Statistical Information

Funds Recommended to Be Put to Better Use		
Reports	**Number of Reports**	**Funds Recommended to Be Put to Better Use**
Audits		
No management decision made by beginning of period[1]	3	$3,051,384
Issued during period	0	$0
Needing management decision during period	3	$3,051,384
Management decisions made during period: – Amounts management agreed to put to better use[2] – Amounts management disagreed to put to better use	 0 3	 $0 $3,051,384
No management decision at end of period	0	$0
Evaluations		
Nothing to report from the Evaluation and Inspections Division.		
Special Reviews		
Nothing to report from the Oversight and Review Division.		

1 Reports previously issued for which no management decision has been made.
2 Includes instances in which management has taken action to resolve the issue and/or the matter is being closed because remedial action was taken.

Statistical Information

Significant Recommendations for Which Corrective Actions Have Not Been Completed			
Report Number and Date	**Report Title**	**Rec. No.**	**Recommendation**
Audits			
Audit Report 07-05 (December 2006)	The Department of Justice's Grant Closeout Process	26	The OIG recommends that the OVW remedy the $37,279,986 in questioned costs related to drawdowns occurring more than 90 days past the grant end date.
		44	The OIG recommends that the OVW deobligate and put to better use the $14,285,431 in remaining funds related to expired grants that are more than 90 days past the grant end date.
Audit Report 10-01 (October 2009)	Explosives Investigation Coordination between the Federal Bureau of Investigation and Bureau of Alcohol, Tobacco, Firearms and Explosives	1	The OIG recommends that the Department implement new directives delineating lead authority for explosives investigations between the FBI and ATF. At a minimum, this guidance should: (1) assign responsibility to either the FBI or ATF to serve as the overall investigational "lead agency" for each specific type of explosives crime; (2) supersede all prior guidance on FBI-ATF explosives coordination; (3) detail actions required to coordinate jointly in circumstances when the motive is unclear. Consideration should be given to whether to divide jurisdiction between the components by device type, defined territories, technical specialization, or reassigning explosives functions and personnel under the provisions of 28 U.S.C. § 599A; and (4) establish a formal procedure for components to seek resolution of jurisdictional conflicts from the Department.

Statistical Information

Evaluations			
I-2010-004 (May 2010)	The Department's Preparation to Respond to a Weapons of Mass Destruction Incident	5	The OIG recommends that the Department ensure that it is prepared to fulfill its emergency support function responsibilities under the National Response Framework, including reviewing the designation of ATF as the Department's lead agency to coordinate public safety and security activities, approving a Concept of Operations Plan, and staffing national and regional coordinator positions.
I-2009-002 (May 2009)	ATF's Project Gunrunner	15	The OIG recommends that ATF ensure that the reforms discussed in their September 2010 document entitled "Project Gunrunner – A Cartel Focused Strategy" are fully and expeditiously implemented.
		6	The OIG recommends that ATF develop a method for Southwest border intelligence personnel to regularly share analytical techniques and best practices pertaining to Project Gunrunner.
Special Reviews[1]			
September 2010	A Review of the FBI's Investigations of Certain Advocacy Groups	3	The OIG recommends that the FBI specify the potential violation of a specific federal criminal statute as part of documenting the basis for opening a preliminary or full investigation in cases involving investigation of advocacy groups or their members for activities connected to the exercise of their First Amendment rights.
March 2007	A Review of the Federal Bureau of Investigation's Use of National Security Letters	2	The OIG recommends that the FBI improve the FBI-OGC NSL tracking database to ensure that it captures timely, complete, and accurate data on NSLs and NSL requests.
May 2006	A Review of the FBI's Handling and Oversight of FBI Asset Katrina Leung	2	The OIG recommends that the FBI should require that any analytical products relating to the asset, together with red flags, derogatory reporting, anomalies, and other counterintelligence concerns be documented in a subsection of the asset's file.

1 Special Reviews do not have report numbers.

Statistical Information

Reports Without Management Decisions for More than 6 Months		
Report Number and Date	**Report Title**	**Report Summary**
Audits		
Nothing to report from the Audit Division.		
Evaluations		
Nothing to report from the Evaluations and Inspections Division.		
Special Reviews[1]		
Nothing to report from the Oversight and Review Division.		

Description and Explanation of the Reasons for Any Significant Revised Management Decision Made During the Reporting Period			
Report Number and Date	**Report Title**	**Rec. No.**	**Recommendation**
Audits			
Nothing to report from the Audit Division.			
Evaluations			
Nothing to report from the Evaluations and Inspections Division.			
Special Reviews[1]			
Nothing to report from the Oversight and Review Division.			

Significant Recommendations in Disagreement for More Than 6 Months			
Report Number and Date	**Report Title**	**Rec. No.**	**Recommendation**
Audits			
Nothing to report from the Audit Division.			
Evaluations			
Nothing to report from the Evaluations and Inspections Division.			
Special Reviews[1]			
Nothing to report from the Oversight and Review Division.			

1 Special Reviews do not have report numbers.

National Defense Authorization Act Reporting

OIG Reporting Required by the *National Defense Authorization Act* for FY 2008

The *National Defense Authorization Act for FY 2008* requires all Inspectors General appointed under the IG Act to add an annex to their Semiannual Reports: (1) listing all contract audit reports issued during the reporting period containing significant audit findings; (2) briefly describing the significant audit findings in the report; and (3) specifying the amounts of costs identified in the report as unsupported, questioned, or disallowed. This Act defines significant audit findings as unsupported, questioned, or disallowed costs in excess of $10 million or other findings that the Inspector General determines to be significant. It defines contracts as a contract, an order placed under a task or delivery order contract, or a subcontract.

The OIG did not issue any audits that fit these criteria during this semiannual reporting period.

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. The Audit Division monitors the status of open audit reports to track the audit resolution and closure process. As of September 30, 2011, the OIG was monitoring the resolution process of 220 open audit reports and closed 102 audit reports this reporting period.

Evaluation and Inspections Workload and Accomplishments

The following chart summarizes the workload and accomplishments of the Evaluation and Inspections Division during the 6-month reporting period ending September 30, 2011.

Evaluation and Inspections Workload and Accomplishments	Number of Reviews
Reviews active at beginning of period	9
Reviews cancelled	0
Reviews initiated	1
Final reports issued	1
Reviews active at end of reporting period	9

Investigations Statistics

The following chart summarizes the workload and accomplishments of the Investigations Division during the 6-month period ending September 30, 2011.

Source of Allegations	
Hotline (telephone, mail, and e-mail)	1,441
Other Sources	4,544
Total allegations received	5,985
Investigative Caseload	
Investigations opened this period	174
Investigations closed this period	210
Investigations in progress as of 9/30/11	362
Prosecutive Actions	
Criminal indictments/ informations	50
Arrests	51
Convictions/Pleas	52
Administrative Actions	
Terminations	17
Resignations	47
Disciplinary action	45
Monetary Results	
Fines/Restitutions/Recoveries/ Assessments/Forfeitures	$3,562,636
Civil Fines/Restitutions/ Recoveries/Penalties/Damages/ Forfeitures	$11,699,367

Investigations Division Briefing Programs

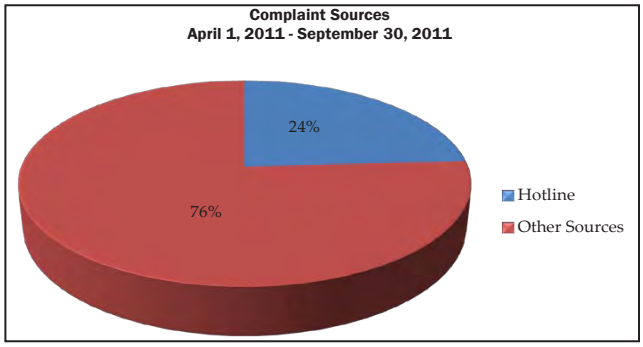
OIG investigators conducted 27 Integrity Awareness Briefings for Department employees throughout the country. These briefings are designed to educate employees about the misuse of a public official's position for personal gain and to deter employees from committing such offenses. The briefings reached more than 835 employees.

OIG Hotline

During FY 2011, the OIG received the majority of its Hotline complaints through its recently modified electronic complaint form located within the OIG website at www.justice.gov/oig.

In addition, Department employees and citizens are able to file complaints by telephone, fax, e-mail, and postal mail. The online access, e-mail, fax, and postal mail all provide the ability to file a complaint in writing to the OIG.

From all Hotline sources during the second half of FY 2011, more than 1,400 new complaints related to department operations or other federal agencies were entered into our complaint tracking system. Of the new complaints, 990 were forwarded to various Department components for their review and appropriate action; 157 were filed for information; 253 were forwarded to other federal agencies, and 8 were opened by the OIG for investigation.



Source: Investigations Data Management System

Appendix 1

Acronyms and Abbreviations

ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
AUSA	Assistant U.S. Attorney
BJA	Bureau of Justice Assistance
BJS	Bureau of Justice Statistics
BOP	Federal Bureau of Prisons
CODIS	Combined DNA Index System
COPS	Office of Community Oriented Policing Services
CSO	Court Security Officer
DEA	Drug Enforcement Administration
Department	U.S. Department of Justice
DHS	Department of Homeland Security
DOD	Department of Defense
EOUSA	Executive Office for U.S. Attorneys
FBI	Federal Bureau of Investigation
FISA	*Foreign Intelligence Surveillance Act of 1978*
FY	Fiscal year
IG Act	*Inspector General Act of 1978*
JMD	Justice Management Division
NDIS	National DNA Index System
NFSTC	National Forensic Science Technology Center
NIJ	National Institute of Justice

Appendices

NSA	National Security Agency
OIG	Office of the Inspector General
OJP	Office of Justice Programs
OJJDP	Office of Juvenile Justice and Delinquency Prevention
OMB	Office on Management and Budget
OPR	Office of Professional Responsibility
OVC	Office for Victims of Crime
OVW	Office on Violence Against Women
Patriot Act	*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*
Recovery Act	*American Recovery and Reinvestment Act of 2009*
SWBPI	Southwest Border Prosecution Initiative
Treasury	Department of the Treasury
UNICOR	Federal Prison Industries
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.

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

Drawdown: The process by which a grantee requests and receives federal funds.

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.

Internal Audit Report: The results of audits and related reviews of Department organizations, programs, functions, computer security and information technology, 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.

***Single Audit Act* Audits:** *Single Audit Act* audits are performed by public accountants or a federal, state or local government audit organization in accordance with generally accepted government auditing standards. They are intended to determine whether the financial statements and schedule of expenditures of federal awards are presented fairly, to test internal controls over major programs, to determine whether the grant recipient is in compliance with requirements that may have a direct and material effect on each of its major programs, and to follow up on prior audit findings. These audits are required to be performed for organizations that expend $500,000 or more in federal awards in accordance with the *Single Audit Act of 1984*, as amended, and Office of Management and Budget (OMB) Circular A-133.

Sole Source Contract: Soliciting and negotiating with only one vendor.

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

Supplanting: For a state or unit of local government to reduce state or local funds for an activity specifically because federal funds are available (or expected to be available) to fund that same activity.

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

Audit Division Reports

Internal Audit Reports

Multicomponent

Status of the Department's Implementation of the Unified Financial Management System

Audit of Department of Justice Conference Planning and Food and Beverage Costs

Audit of the Department of Justice Processing of Clemency Petitions

Audit of the Justice Security Operations Center's Capabilities and Coordination

Bureau of Alcohol, Tobacco, Firearms and Explosives

Audit of the Bureau of Alcohol, Tobacco, Firearms and Explosives' Information Security Program Pursuant to the *Federal Information Security Management Act* FY 2010

Audit of the Bureau of Alcohol, Tobacco, Firearms and Explosives' National Field Office Case Information System Pursuant to the *Federal Information Security Management Act* FY 2010

Drug Enforcement Administration

Audit of the Drug Enforcement Administration's Information Security Program Pursuant to the *Federal Information Security Management Act* FY 2010

Audit of the Drug Enforcement Administration's Intelligence Research Support System Pursuant to the *Federal Information Security Management Act* FY 2010

Federal Bureau of Investigation

Audit of the Federal Bureau of Investigation's Bureau Investigative Document Management and Analysis System Pursuant to the *Federal Information Security Management Act* FY 2010

Audit of the Federal Bureau of Investigation's Convicted Offender, Arrestee, and Detainee DNA Backlog

Audit of the Federal Bureau of Investigation's Cryptanalysis Initiative Computer Net System Pursuant to the *Federal Information Security Management Act* FY 2010

Audit of the Federal Bureau of Investigation's Security Program Pursuant to the *Federal Information Security Management Act* FY 2010

The Federal Bureau of Investigation's Ability to Address the National Security Cyber Intrusion Threat

Office of Justice Programs

Audit of the Office of Justice Programs' Information Security Program Pursuant to the *Federal Information Security Management Act* FY 2010

Audit of the Office of Justice Programs' National Criminal Justice Reference Service System Pursuant to the *Federal Information Security Management Act* FY 2010

U.S. Marshals Service

Audit of the United States Marshals Service Complex Asset Team Management and Oversight

Other Department Components

Audit of Superfund Activities in the Environment and Natural Resources Division for FYs 2009 and 2010

Audit of the Executive Office for United States Attorneys' Case Management Enterprise System Pursuant to the *Federal Information Security Management Act* FY 2010

Audit of the Executive Office for United States Attorneys' Information Security Program Pursuant to the *Federal Information Security Management Act* FY 2010

Audit of the Justice Management Division's Information Security Program Pursuant to the *Federal Information Security Management Act* FY 2010

Audit of the Justice Management Division's Justice Consolidated Office Network-Secret Pursuant to the *Federal Information Security Management Act* FY 2010

Audit of the National Security Division's NSDNet-S System Pursuant to the *Federal Information Security Management Act* FY 2010

Audit of the National Security Division's Information Security Program Pursuant to the *Federal Information Security Management Act* FY 2010

Audit of the United States National Central Bureau of Interpol's Information Security Program Pursuant to the *Federal Information Security Management Act* FY 2010

Audit of the United States National Central Bureau of Interpol's OA/Envoy System Pursuant to the *Federal Information Security Management Act* FY 2010

Appendices

External Reports

Alabama

Audit of Office of Justice Programs Edward Byrne Memorial Justice Assistance Grants Awarded to the City of Birmingham, Alabama

Arizona

Audit of Compliance with Standards Governing Combined DNA Index System Activities at the Tucson Police Department Crime Laboratory, Tucson, Arizona

California

Audit of the COPS Grant Awarded to the Corcoran Police Department, Corcoran, California

Audit of the Office of Justice Programs Edward Byrne Memorial Justice Assistance Grant Program Grants Awarded to the City of Suisun City, California

District of Columbia

Audit of the Office of Justice Programs Office of Juvenile Justice and Delinquency Prevention Awards to the Best Friends Foundation, Washington, D.C.

Florida

Audit of the COPS Technology Grant Awarded to the Cape Coral Police Department, Cape Coral, Florida

Indiana

Limited Scope Audit of the Coalition Against Domestic Abuse, Incorporated, Knox, Indiana

Maryland

Audit of Montgomery County Department of Police Equitable Sharing Program Activities, Rockville, Maryland

Massachusetts

Audit of the Office on Violence Against Women Grants to Jane Doe, Inc., Boston, Massachusetts

Michigan

Audit of COPS 2007 Technology Program Grant Awarded to the Township of Kalamazoo, Michigan

Audit of the Office of Justice Programs National Institute of Justice Cooperative Agreement Awarded to Occupational Research and Assessment, Incorporated, Big Rapids, Michigan

Minnesota

Limited Scope Audit of the Saint Paul, Minnesota, Police Department

Missouri

Audit of the Office of Justice Programs National Institute of Justice Grant Awarded to the Jackson County Medical Examiner's Office, Kansas City, Missouri

New Mexico

Audit of Office of Community Oriented Policing Services Technology Program Grants Awarded to the City of Albuquerque, New Mexico

Ohio

Audit of the Use of Equitable Sharing Revenues by the Cleveland Police Department, Cleveland, Ohio

Audit of Compliance with Standards Governing Combined DNA Index System Activities at the Ohio Bureau of Criminal Identification and Investigation, London, Ohio

Oregon

Audit of the Office of the Community Oriented Policing Services Grant Awarded to the Sherwood Police Department, Sherwood, Oregon

South Carolina

Limited Scope Audit of the Office of Justice Programs Victims of Crime Act Grants to the South Carolina Department of Public Safety Sub-Awarded to Safe Passage, Inc., Rock Hill, South Carolina

Tennessee

Audit of Compliance with Standards Governing Combined DNA Index System Activities at the Tennessee Bureau of Investigation Memphis Regional Crime Laboratory, Memphis, Tennessee

Texas

Audit of Denton County Texas Sheriff's Office Equitable Sharing Program Activities, Denton, Texas

Audit of Compliance with Standards Governing Combined DNA Index System Activities at the Texas Department of Public Safety Lubbock Criminal Laboratory, Lubbock, Texas

Audit of Compliance with Standards Governing Combined DNA Index System Activities at the Texas Department of Public Safety McAllen Criminal Laboratory, McAllen, Texas

Audit of Compliance with Standards Governing Combined DNA Index System Activities at the Tarrant County Medical Examiner's Office Tarrant County, Texas

Audit of the Office of Justice Programs Grants Awarded to the University of North Texas Health Science Center, Forth Worth, Texas

Virginia

Audit of the Office of Justice Programs Office of Juvenile Justice and Delinquency Prevention Awards to Enough is Enough, Reston, Virginia

Washington

Audit of the Office of Justice Programs Rural Law Enforcement Assistance Grant Awarded to the City of Aberdeen, Washington

Wisconsin

Limited Scope Audit of the Office of Justice Programs Bureau of Justice Assistance Grant Awarded to Safe & Sound, Incorporated, Milwaukee, Wisconsin

Single Audit Act Reports of Department Activities

A Child is Missing, Incorporated, Fort Lauderdale, Florida, FY 2009

City of Brea, California, FY 2010

Chatham County, Georgia, FY 2010

Domestic Violence Action Center, Honolulu, Hawaii, FY 2009

City of Doraville, Georgia, FY 2010

East Bay Regional Communication Systems Authority, Dublin, California, FY 2010

Illinois Coalition Against Sexual Assault, Springfield, Illinois, FY 2010

Johnson County, Indiana, FY 2009

Los Angeles Interagency Metropolitan Police Apprehension Crime Task Force, FY 2010

National Alliance for Drug Endangered Children, Westminster, Colorado, FY 2008

National Center for Victims of Crime, Washington D.C., FY 2009

City of North Miami Beach, Florida, FY 2008

Operation QT, Incorporated, Phoenix, Arizona, FY 2010

Riverside Christian Ministries, Incorporated, Miami, Florida, FY 2010

Appendix 4

Quantifiable Potential Monetary Benefits

October 1, 2010 – March 31, 2011

Audit Report	Questioned Costs	Unsupported Costs	Funds Put to Better Use
Audits Performed by the DOJ OIG			
Audit of Department of Justice Conference Planning and Food and Beverage Costs	$134,432	$0	$0
Audit of Superfund Activities in the Environment and Natural Resources Division for FYs 2009 and 2012	$27,966	$0	$0
Audit of Office of Justice Programs Edward Byrne Memorial Justice Assistance Grants Awarded to the City of Birmingham, Alabama	$2,513	$0	$0
Audit of the Office of Community Oriented Policing Services Grant Awarded to the Corcoran Police Department, Corcoran, California	$321,829	$249,734	$0
Audit of the Office of Justice Programs Office of Juvenile Justice and Delinquency Prevention Awards to the Best Friends Foundation, Washington, D.C.	$182,881	$164,985	$0
Audit of Montgomery County Department of Police Equitable Sharing Program Activities, Rockville, Maryland	$20,199	$0	$0
Audit of the Office on Violence Against Women Grants to Jane Doe, Inc., Boston, Massachusetts	$638,298	$605,504	$0
Audit of the Office of Justice Programs National Institute of Justice Cooperative Agreement Awarded to Occupational Research and Assessment, Incorporated, Big Rapids, Michigan	$138,310	$138,310	$0
Audit of Office of Community Oriented Policing Services Technology Program Grants Awarded to the City of Albuquerque, New Mexico	$99,423	$0	$0

Audit of the Use of Equitable Sharing Revenues by the Cleveland Police Department, Cleveland, Ohio	$5,971	$0	$0
Audit of Denton County Texas Sheriff's Office Equitable Sharing Program Activities, Denton, Texas	$5,176	$5,176	$0
Audit of the Office of Justice Programs Grants Awarded to the University of North Texas Health Science Center, Forth Worth, Texas	$130,733	$0	$0
Audit of the Office of Justice Programs Office of Juvenile Justice and Delinquency Prevention Awards to Enough is Enough, Reston, Virginia	$801,357	$795,637	$0
Audit of the Office of Justice Programs Rural Law Enforcement Assistance Grant Awarded to the City of Aberdeen, Washington	$9,563	$9,563	$0
Limited Scope Audit of the Office of Justice Programs Bureau of Justice Assistance Grant Awarded to Safe & Sound, Incorporated, Milwaukee, Wisconsin	$41,771	$0	$0
Subtotal (Audits Performed by the DOJ OIG)	**$2,560,422**	**$1,968,909**	**$0**
Audits Performed by State/Local Auditors and Independent Public Accounting Firms Under the *Single Audit Act*[1]			
City of Brea, California FY 2010	$34,362	$0	$0
Operation Quality Time, Incorporated, Phoenix, Arizona FY 2010	$120,422	$0	$0
Riverside Christian Ministries, Incorporated, Miami, Florida FY 2010	$35,000	$0	$0
Subtotal (Audits Performed by State/Local Auditors and Independent Public Accounting Firms Under the *Single Audit Act*)	**$189,784**	**$0**	**$0**
Total	**$2,750,206**	**$1,968,909**	**$0**

1 These audits are reviewed by the OIG to assess the quality and the adequacy of the entity's management of federal funds. The OIG issues these audits to the responsible component and performs follow-up on the audit reports' findings and recommendations.

Appendix 5

Evaluation and Inspections Division Reports

Enhanced Screening of BOP Correctional Officer Candidates Could Reduce Likelihood of Misconduct

Oversight and Review Division Reports

A Review of the FBI's Progress in Responding to the Recommendations in the OIG's Report on the Fingerprint Misidentification in the Brandon Mayfield Case

Appendix 6

Peer Reviews

Peer Reviews Conducted by Another OIG

The OIG did not undergo any peer reviews this semiannual reporting period. The most recent peer review of the Audit Division was issued on February 26, 2010, by the Department of Energy OIG. The most recent peer review of the investigative function was January 2010 by the Department of Health and Human Services OIG.

Outstanding Recommendations from Peer Reviews of the OIG

There are no outstanding recommendations from peer reviews of the OIG.

Outstanding Recommendations from Peer Reviews Conducted by the OIG

In May 2011, members of the Department's OIG conducted a review of the internal safeguards and management procedures for the investigative function of the U.S. Postal Service (USPS) OIG in effect for the period ending March 31, 2011. The review was conducted in conformity with the quality assessment review guidelines established by the *Council of Inspectors General on Integrity and Efficiency* (CIGIE) and the Attorney General's Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority, as applicable. The review was conducted at the USPS OIG Headquarters Office in Arlington, Virginia, and two field office locations in Atlanta, Georgia, and Chicago, Illinois. A total of 50 investigative case files were sampled.

The Department's OIG concluded that the system of internal safeguards and management procedures for the investigative function of the USPS OIG investigative function in effect for the period ending March 31, 2011, was in full compliance with the quality standards established by CIGIE and the Attorney General's guidelines. These safeguards and procedures provide reasonable assurance of conforming with professional standards in the conduct of its investigations.

Agency Reviewed by the Department's OIG	Functional Area	Recommendations	Date Issued
U.S. Postal Service OIG	Investigations	No recommendations were made	6/20/11

Appendix 7

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	53
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	9-50
Section 5(a)(2)	Significant Recommendations for Corrective Actions	9-50
Section 5(a)(3)	Significant Recommendations for Which Corrective Actions Have Not Been Completed	57-58
Section 5(a)(4)	Matters Referred to Prosecutive Authorities	14, 22-23, 28-29, 32-33, 35, 37-38, 40-41, 43, 45, 47-48, 50
Section 5(a)(5)	Refusal to Provide Information	None
Section 5(a)(6)	Listing of Audit Reports	67-71
Section 5(a)(7)	Summary of Significant Reports	9-50
Section 5(a)(8)	Questioned Costs	55
Section 5(a)(9)	Funds Recommended to Be Put to Better Use	56
Section 5(a)(10)	Reports Without Management Decisions for More than 6 Months	59
Section 5(a)(11)	Description and Explanation of the Reasons for Any Significant Revised Management Decision Made During the Reporting Period	59
Section 5(a)(12)	Significant Recommendations in Disagreement for More than 6 Months	59
Section 5(a)(14)	Peer Reviews Conducted by Another OIG	75
Section 5(a)(15)	Outstanding Recommendations from Peer Reviews of the OIG	75
Section 5(a)(16)	Outstanding Recommendations from Peer Reviews Conducted by the OIG	75

Report Waste, Fraud, Abuse, or Misconduct

To report allegations of waste, fraud, abuse, or misconduct regarding Department of Justice programs, employees, contractors, or grants, please go to the website of the DOJ OIG at www.justice.gov/oig or call the OIG's Hotline at (800) 869-4499.

The OIG website has complaint forms that allow you to report the following to the OIG:

- General allegations of fraud, waste, and abuse in Department programs or by Department employees;
- Contract fraud, including mandatory disclosures required by contractors when they have credible evidence of violations of the civil False Claims Act or certain violations of criminal law;
- Grant fraud, including fraud, waste, or abuse related to the Department's award of Recovery Act funds; and
- Violations of civil rights or civil liberties by Department employees.

To submit information by mail or facsimile, please send to:

Office of the Inspector General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Room 4706
Washington, DC 20530
Fax: (202) 616-9881

For further information on how to report a complaint to the OIG, please call (800) 869-4499.

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