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

Office of the Inspector General Semiannual Report to Congress

October 1, 2006 – March 31, 2007

Message From the Inspector General

This was a busy and productive semiannual period for the Office of the Inspector General (OIG). Our audits, investigations, inspections, and special reviews continued to have an important impact on Department of Justice (Department) programs and operations.

The OIG issued two reviews required by the *USA Patriot Improvement and Reauthorization Act of 2005* (Patriot Reauthorization Act) that examined the Federal Bureau of Investigation's (FBI) use of national security letters (NSL) and Section 215 orders to obtain business records. Our report on Section 215 orders did not find improper uses of that authority. However, our report on NSLs found significant problems in the FBI's use of these letters, including inaccurate reporting to Congress on the number of letters issued by the FBI as well as a significant number of misuses of these letters. We are continuing to review the FBI's use of NSLs and Section 215 orders and are monitoring the FBI's corrective measures to address the problems that our review of NSLs identified.

We also conducted other noteworthy reviews and investigations. For example we issued reports examining the Department's reporting of terrorism statistics, the Department's attempts to develop an Integrated Wireless Network that would permit federal law enforcement officers to communicate across agencies, the Department's grant close-out process, the Drug Enforcement Administration's (DEA) handling of cash seizures, the FBI's control over its weapons and laptop computers, and the FBI's efforts to develop its Sentinel electronic case management system. In addition, our Investigations Division handled sensitive criminal and administrative investigations of misconduct related to Department programs and operations.

The OIG also began a review of the Department's involvement with the National Security Agency's (NSA) program called the "terrorist surveillance program" or "warrantless surveillance program." In addition, the OIG initiated a joint investigation with the Department's Office of Professional Responsibility to examine issues related to the recent removal of several U.S. Attorneys.

During this period, the Department organized the National Procurement Fraud Task Force, which seeks to prevent, detect, and prosecute procurement and grant fraud. As part of that effort, the OIG is chairing the Grant Fraud Committee of the task force. We believe this task force and the Grant Fraud Committee are important initiatives that can help detect and deter fraud that can be committed with the billions of dollars in grants and contracts that the Department issues each year.

Finally, I want to express my appreciation for the cooperation and support we regularly receive from the Department and Congress. I also want to recognize the extraordinary dedication and professionalism of the OIG's staff. With limited resources, the OIG has completed a wide range of significant reports and investigations, and OIG employees deserve great credit for their hard work.

Glenn A. Fine
Inspector General
April 30, 2007

Table of Contents

Highlights of OIG Activities

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

Statistical Highlights

October 1, 2006 – March 31, 2007

Allegations Received by the Investigations Division	4,529
Investigations Opened	201
Investigations Closed	203
Arrests	35
Indictments/Informations	36
Convictions/Pleas	64
Administrative Actions	87
Fines/Restitutions/Recoveries	$663,907
Audit Reports Issued	106
Questioned Costs	$560 million
Funds Put to Better Use	$170 million
Recommendations for Management Improvements	420

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

- **The FBI's Use of National Security Letters and Section 215 Authorities.** The Patriot Reauthorization Act directed the OIG to review the FBI's use of national security letters (NSL) and Section 215 orders to obtain business records. Our review of NSLs from 2003 through 2005 found that the FBI's use of NSL authorities has increased dramatically since the enactment of the *USA Patriot Act* (Patriot Act) in October 2001. We also found that the Department's reports to Congress on NSL usage significantly understated the total number of NSL requests. The OIG review found serious and widespread misuse of NSL authorities, such as issuing NSLs without proper authorization, making improper requests under the statutes cited in the NSLs, and conducting unauthorized collection of telephone or Internet e-mail transactional records. In addition, the OIG review identified more than 700 instances in which the FBI improperly obtained telephone toll billing records and subscriber information by issuing "exigent letters" rather than by issuing NSLs. The OIG made 10 recommendations to the FBI related to its use of NSLs. The FBI concurred with our recommendations and agreed to implement corrective actions.

  With respect to the FBI's use of Section 215 authorities, our review did not identify any instances involving improper or illegal use in connection with "pure" Section 215 orders. We also found that the FBI did not obtain Section 215 orders for any library records during the time period covered by our review. However, the OIG found significant delays within the FBI and the Department in processing requests for Section 215 orders, and that the FBI had not used Section 215 orders as effectively as it could have because of legal, bureaucratic, or other impediments to obtaining these orders.

- **Development of the Department's Integrated Wireless Network.** The OIG audited the progress of the Integrated Wireless Network (IWN), an approximately $5 billion joint project between the Department and the Departments of Homeland Security (DHS) and Treasury that is intended to address federal law enforcement requirements to communicate across agencies, allow interoperability with state and local law enforcement partners, and meet mandates to use federal radio frequency spectrum more efficiently. The OIG review concluded that the IWN project is at high risk of failure, and the partnership between the Department and the DHS is fractured. As a result, despite over 6 years of development and more than $195 million in funding, the IWN project does not appear to be on the path to providing the seamless interoperable communications system that was envisioned. The causes for the high risk of project failure include uncertain and disparate funding mechanisms for IWN, the fractured IWN partnership, and the lack of an effective governing structure for the project.

- **The FBI's Control Over Weapons and Laptop Computers.** The OIG issued a follow-up audit of the FBI's efforts to improve controls over its weapons and laptop computers. Since our initial report in 2002, we found that the FBI has made progress in decreasing the rate of loss for its weapons and laptops. However, we determined that at least 10 of the 160 laptops reported missing or stolen during the 44-month review period covered by this audit contained sensitive or classified information, and the FBI could not determine whether 51 additional lost or stolen laptops contained sensitive or classified information. Although the FBI has improved its controls since our previous audit by establishing deadlines for reporting lost and stolen weapons and laptops, entering those losses into the National Crime Information Center, and referring the losses for investigation, FBI personnel have not consistently followed these procedures. We made 13 recommendations to the FBI to improve its management controls over weapons and laptops. In response, the FBI has outlined a plan for taking corrective action to address all of our recommendations.

- **The Department's Internal Controls Over Terrorism Reporting.** Several components, including the FBI, Criminal Division, and Executive Office for U.S. Attorneys (EOUSA), collect terrorism-related statistics to help measure the Department's counterterrorism efforts. The OIG audited the accuracy of 26 terrorism-related statistics issued by these 3 Department components and found that all but 2 of the 26 statistics were inaccurate. Some were overstated and some were understated. We also found that the Department's collection and reporting of these statistics was decentralized and haphazard. The OIG made six recommendations to help improve the accuracy of these statistics. The FBI agreed with all of our recommendations, the Criminal Division agreed with all but one of our recommendations, and EOUSA disagreed with our recommendations.

- **Critical Incident Response Plans.** The OIG issued a follow-up report to our 2003 review of U.S. Attorneys' Offices (USAO) Critical Incident Response Plans, which are used to ensure that USAOs are ready to respond to major incidents such as acts of terrorism, hostage situations, and natural disasters. Our follow-up review found that the Department, in response to the recommendations in our 2003 audit, has taken important steps to improve USAOs' preparedness to respond in an emergency. However, many USAOs have regressed in their required Critical Incident Response Plan activities. We made seven recommendations to help the Department continue to improve USAOs' ability to respond quickly and appropriately to critical incidents.

The Department concurred with all of our recommendations.

- **The DEA's Handling of Cash Seizures.** The OIG audited the DEA's handling of cash that it seizes during its investigations. We found that the DEA failed to consistently follow or document compliance with its policies for handling and safeguarding seized cash. The OIG made seven recommendations to improve the DEA's handling of seized cash, and the DEA agreed with all but one of our recommendations.

- **The Department's Grant Closeout Process.** The OIG audited the process used by the Department to close out the billions of dollars in grants that it distributes annually to state, local, and tribal governments and other organizations. We found that timely grant closeout continues to be a significant problem within the Department. Only 13 percent of the 60,933 grants in our sample were closed within 6 months after the grant end date, as required by Office of Justice Programs (OJP) and Office on Violence Against Women (OVW) policy. We also identified a backlog of over 12,000 expired grants more than 6 months past the grant end date that had not been closed, of which 67 percent had been expired for more than 2 years. We made 44 recommendations to improve the grant closeout process, and the Department components agreed with the majority of our recommendations.

- **Development of the FBI's Sentinel Case Management System.** The OIG's second report auditing the FBI's ongoing development of its Sentinel information technology (IT) project found that the FBI has made significant progress in addressing several important areas reported in our first audit of Sentinel. However, we identified several issues that we believe the FBI should continue to address as the Sentinel project moves through its first phase of development and enters its more challenging and higher-risk second phase in early 2007. Although we found that the FBI has taken a positive step by establishing a risk management plan that identifies the significant risks associated with the Sentinel project, we also determined that contingency plans, and the triggers for activating such plans, exist for only 3 of the 20 identified risks being monitored. The FBI agreed with our recommendations.

Investigations

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

- Sentencing has been imposed on five of the six Federal Bureau of Prisons (BOP) correctional officers who were charged with conspiracy to sexually abuse female inmates and introduction of contraband into the BOP facility. This is the case in which OIG Special Agent William "Buddy" Sentner III was shot and killed on June 21, 2006, when the correctional officers were being arrested. The first of the two correctional officers who pled guilty received 12 months' incarceration followed by 3 years' supervised release, and the second received probation. Two other correctional officers were convicted at trial on charges of bribery and witness tampering. One was sentenced to 12 months' incarceration and 3 years' supervised release and fined $6,000, while the other was sentenced to 12 months' incarceration and 3 years' supervised release and fined $3,000. The fifth correctional officer pled guilty to conspiracy charges and was sentenced to 36 months' probation and 12 months' home confinement. The sixth

correctional officer was killed in the exchange of gunfire that he initiated.

- The former Mayor of Fairbanks, Alaska, and his wife were arrested pursuant to a 92-count indictment charging them with theft of $450,000 in federal grant funds, conspiracy, and money laundering. A joint investigation in which the OIG participated concluded that they misappropriated federal grant funds designated to operate a non-profit organization by using them for personal reasons, including to partially fund the building of their church.

- An FBI Special Agent was terminated from his position after an OIG investigation determined that he provided unauthorized disclosure of a document classified "Secret" and divulged the existence of an FBI search warrant prior to its execution to a female journalism student with whom he had a 2-year extramarital relationship.

- A BOP correctional officer assigned to the U.S. Penitentiary in Atwater, California, was sentenced to 37 months' incarceration and 36 months' supervised release pursuant to his guilty plea to a charge of possession of heroin with intent to distribute. During an undercover operation with OIG and DEA investigators, the correctional officer accepted 5 ounces of black tar heroin and a $5,000 bribe to smuggle the heroin into the penitentiary.

- A DEA contracting officer was arrested and charged with corruptly profiting from his employment as a federal agent and making a false statement after a joint OIG and DEA Office of Professional Responsibility investigation developed evidence that he personally received $13,442 from a DEA vendor whose contract he managed.

- An OIG investigation led to the arrest and guilty plea by a recipient of a Department grant for theft of government program funds. The investigation found that the Comptroller for the American Prosecutors Research Institute embezzled $76,464 in OJP grant funds.

Ongoing Work

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

- Review of the Department's involvement with the NSA program known as the "terrorist surveillance program" or "warrantless surveillance program"

- FBI reports relating to alleged abuse of military detainees at Guantanamo and other facilities

- Coordination of violent crime task forces in the Department

- The Department's removal of U.S. Attorneys

- Follow-up reviews of the FBI's use of national security letters and Section 215 orders

- Follow-up review on the FBI's response to recommendations made in the Robert Hanssen review

- Follow-up review of the Terrorist Screening Center

- The FBI's efforts to combat crimes against children

- The FBI's progress in hiring, training, and retaining intelligence analysts

- Follow-up review of the U.S. Marshals Service's (USMS) efforts to provide judicial security

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, DEA, BOP, USMS, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), USAO, and all other organizations within the Department, as well as contractors of the Department and organizations receiving grant money from the Department.

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

- **Audit Division** is responsible for independent audits of Department programs, computer systems, and financial statements. The Audit Division has field offices in Atlanta, Chicago, Dallas, Denver, Philadelphia, San Francisco, and Washington, D.C. Its Financial Statement Audit Office and Computer Security and Information Technology Audit Office are located in Washington, D.C. Audit Headquarters consists of the immediate office of the Assistant Inspector General for Audit, the Office of Operations, the Office of Policy and Planning, and an Advanced Audit Techniques Group.
- **Investigations Division** is responsible for investigating allegations of bribery, fraud, abuse, civil rights violations, and violations of other criminal laws and administrative procedures governing Department employees, contractors, and grantees. The Investigations Division has field offices in Chicago, Dallas, Denver, Los Angeles, Miami, New York, and Washington, D.C. The Fraud Detection Office is located in Washington, D.C. The Investigations Division has smaller, area offices in Atlanta, Boston, Detroit, El Paso, Houston, Philadelphia, San Francisco, and Tucson. Investigations Headquarters in Washington, D.C., consists of the immediate office of the Assistant Inspector General for Investigations and the following branches: Operations, Special Operations, Investigative Support, Research and Analysis, and Administrative Support.
- **Evaluation and Inspections Division** conducts program and management reviews that involve on-site inspection, statistical analysis, and other techniques to review Department programs and activities and make recommendations for improvement.
- **Oversight and Review Division** blends the skills of attorneys, investigators, program analysts, and paralegals to review Department programs and investigate sensitive allegations involving Department employees and operations.
- **Management and Planning Division** provides advice to OIG senior leadership on

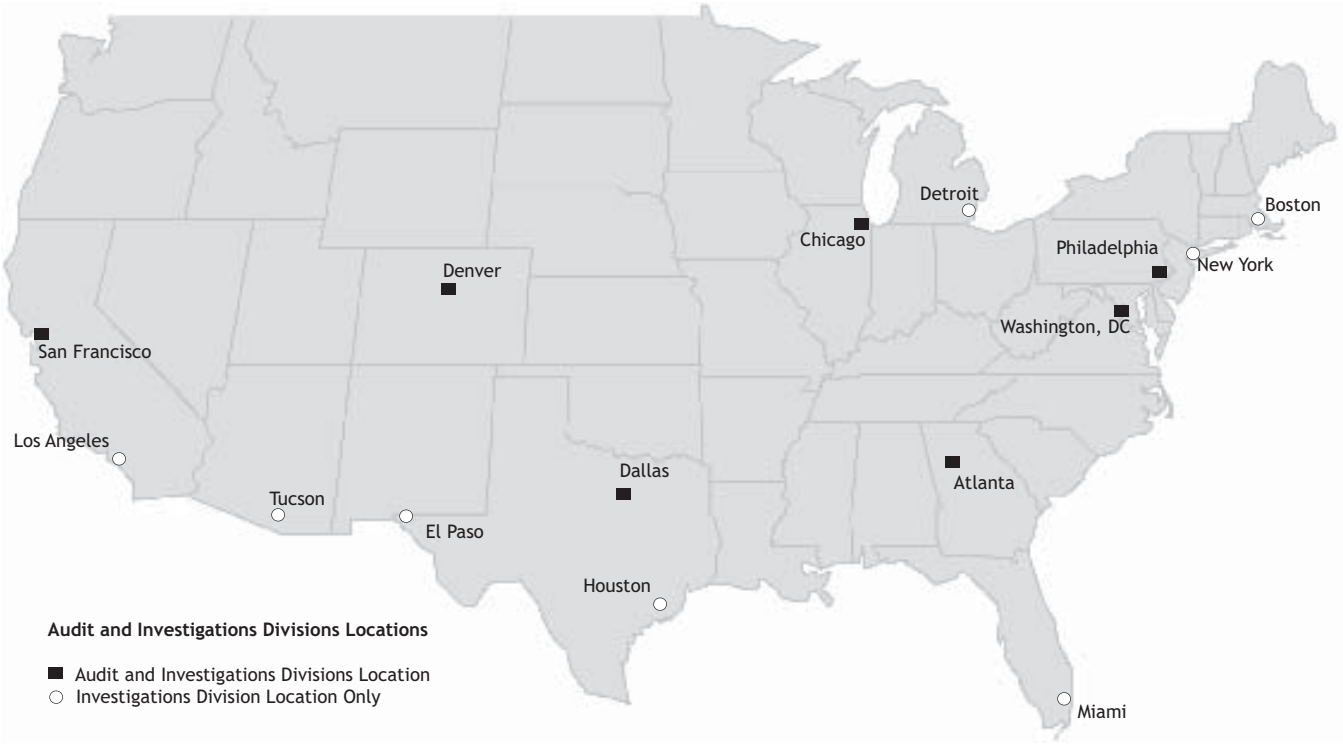
administrative and fiscal policy and assists OIG components in the areas of budget formulation and execution, security, personnel, training, travel, procurement, property management, information technology, computer network communications, telecommunications, quality assurance, internal controls, and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

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

The OIG has a nationwide workforce of approximately 400 Special Agents, auditors, inspectors, attorneys, and support staff. For fiscal year (FY) 2006, the OIG's direct appropriation was $68 million, and the OIG expects to receive an additional $3.3 million in reimbursements.

As required by Section 5 of the *Inspector General Act of 1978*, as amended, this *Semiannual Report to Congress* reviewing the accomplishments of the OIG for the 6-month period of October 1, 2006, through March 31, 2007, is to be submitted no later than April 30, 2007, to the Attorney General for his review. The Attorney General is required to forward the report to Congress no later than May 31, 2007, along with information on the Department's position on audit resolution and follow-up activity in response to matters discussed in this report.

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



Multicomponent Audits, Reviews, and Investigations

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

Reports Issued

Progress Report on the Development of the Department's Integrated Wireless Network

The OIG's Audit Division audited the progress made toward developing the Integrated Wireless Network (IWN), an approximately $5 billion joint project between the Department, DHS, and Treasury Department. IWN is intended to address federal law enforcement requirements to communicate across agencies, allow interoperability with state and local law enforcement partners, and meet mandates to use federal radio frequency spectrum more efficiently. When fully implemented, IWN is intended to support approximately 81,000 federal agents and officers in all 50 states and U.S. territories. For the Department's law enforcement officers, IWN is intended to replace antiquated and functionally limited communications systems.

The OIG determined that IWN is at high risk of failure and the partnership between the Department and the DHS is fractured. As a result, despite over 6 years of development and more than $195 million in funding, the IWN project does not appear to be on the path to providing the seamless interoperable communications system that was envisioned.

The causes for the high risk of project failure include uncertain and disparate funding mechanisms for IWN, the fractured IWN partnership, and the lack of an effective governing structure for the project. In addition, our assessment indicated that a major infusion of funding will be required over the next several years if the involved agencies are to complete IWN as planned. The Department has expressed concern, however, that the DHS has not always lived up to its commitments to IWN, in part because of funding differences. In particular, the Department is required to develop a department-wide wireless program, while the DHS has separate funding for IWN and its legacy communications systems, which allows the DHS to meet the immediate needs of its components by replacing and upgrading legacy communications systems separately from participating in IWN. The OIG also found that the current governing structure for the IWN project is ineffective and has led to significant delays in the program.

As a result, the Department has spent increasingly significant amounts of money to maintain its

legacy communications systems, thereby depleting available funding for IWN.

In addition, the failure of IWN could have significant adverse consequences even beyond the financial losses. It could affect the safety of Department law enforcement officers because the Department's legacy communications systems have limited functionality, diminished voice quality, and weak security, making them vulnerable to hacking. In addition, the Department systems are subject to interference from narrowband communications from other agencies.

Moreover, the differences in approach between the Department and the DHS may result in communications systems that are not well coordinated. The resulting systems may not reflect the seamless communications capability that IWN was originally intended to achieve, and they may not be adequate in the event of future terrorist attacks or natural disasters.

The OIG made four recommendations to help ensure that this important project does not fail. In particular, we recommended that the Department reach an agreement with the DHS and Treasury Department explicitly stating the shared goals, responsibilities, and resource contributions and funding requirements of the sponsoring departments. The Department agreed with all of our recommendations.

The Department's Internal Controls Over Terrorism Reporting

Several components, including the FBI, Criminal Division, and EOUSA, collect terrorism-related statistics to help measure the Department's counterterrorism efforts. These statistics are reported to senior Department managers, Congress, and the public in various reports, budget documents, and testimony. The OIG's Audit Division audited the accuracy of 26 terrorism-related statistics published by these Department components. Among the statistics we reviewed were the number of terrorism threats tracked by the FBI in FYs 2003 and 2004; the number of terrorism convictions reported by EOUSA during FYs 2003 and 2004; and the number of individuals convicted or who pled guilty resulting from terrorism convictions from September 11, 2001, to February 3, 2005, as reported by the Criminal Division.

Our review determined that all but 2 of the 26 statistics were inaccurate. Specifically, we found that 11 were under-reported, 10 were over-reported, 2 were accurately reported, and 3 were reported multiple times. Most of the statistics the OIG tested were significantly overstated or understated, while a few were overstated or understated by minor amounts. Of the statistics the OIG tested, EOUSA inaccurately reported all 11 statistics, the Criminal Division inaccurately reported all 5 statistics, and the FBI inaccurately reported 8 of the 10 statistics.

We found that the statistics were inaccurately reported for a variety of reasons, including that the components could not provide support for the numbers reported, could not provide support for a terrorism link used to classify statistics as terrorism-related, and could not document that the activity reported occurred in the period reported. We also found that the Department's collection and reporting of terrorism-related statistics was decentralized and haphazard. For many of the statistics, Department officials either had not established internal controls to ensure the statistics were accurately gathered, classified, and reported or did not document the internal controls used.

In our review of the statistics, we looked for and accepted any terrorism linkage whether in writing or expressed orally by Department officials.

However, we found many cases involving offenses such as immigration violations, marriage fraud, or drug trafficking where Department officials provided no evidence to link the subject of the case to terrorist activity.

In response to the report, EOUSA noted that the OIG interpreted its antiterrorism program category code definition to require that defendants in antiterrorism cases have an identifiable link to terrorist activity. EOUSA claimed that this interpretation would not capture a much broader group of proactive cases that it claimed have been affirmatively and intentionally brought to deter and prevent terrorism, particularly in the areas of critical infrastructure vulnerability, regardless of whether the defendant has any links to terrorist activity. In support of its argument, EOUSA pointed to cases such as those from Operation Tarmac, an enforcement operation launched in November 2001 at some of the nation's airports that resulted in convictions of many airport workers on a variety of charges, including immigration violations. EOUSA also argued that all convictions in investigations worked by Joint Terrorism Task Forces (JTTFs), regardless of the ultimate findings in the case, should be included as examples of antiterrorism cases.

However, the OIG determined that even giving credit for all JTTF cases and Operation Tarmac and similar cases, EOUSA's statistics remained largely inaccurate. The OIG also disagreed that all convictions in cases like Operation Tarmac should be counted as antiterrorism convictions, given EOUSA's current definition of its antiterrorism program category. The OIG recognized that while efforts like Operation Tarmac may be intended to deter potential terrorists, as well as a wide range of other criminal activity, including all convictions resulting from the operation under EOUSA's anti-terrorism category – without explanation – does not clearly provide full information to Congress and the public about EOUSA's statistics.

The OIG also found that an investigative lead pursued by JTTF may clear the defendant of any connection to terrorism, while finding and convicting the subject of other criminal activity. The OIG concluded that including all such convictions as "antiterrorism convictions" simply because a JTTF pursued the investigation results in inaccurate and misleading statistics.

In response to the OIG's report, EOUSA agreed to rename its antiterrorism program category and modify and clarify its definition in order to eliminate any misunderstanding regarding its meaning. In total, the OIG made six recommendations to assist the FBI, Criminal Division, and EOUSA in improving the accuracy of its reported terrorism-related statistics, including for components to maintain documentation to identify the source of all terrorism-related statistics reported and document the procedures and systems used to gather or track the statistics reported. The FBI agreed with all of our recommendations, the Criminal Division agreed with all but one of our recommendations, and EOUSA disagreed with our recommendations.

The Department's Grant Closeout Process

The OIG's Audit Division audited the process used by the Department to close out the billions of dollars in grants that it distributes annually to state, local, and tribal governments and other organizations. Timely grant closeout is an essential management practice because it can identify grantees that have failed to comply with grant requirements, identify excess and unallowable costs charged to the grant, and identify unused funds that can be deobligated and used for other grants. Prior OIG audit reports have raised significant concerns related to grant closeout and grant oversight procedures within the Department. As a result, grant management

has been listed by the OIG as one of the Department's top 10 management challenges for the past 6 years.

In this audit, we examined 44,197 grants totaling $17.61 billion that were closed from October 1997 to December 2005 and 16,736 expired grants totaling $7.41 billion that had not been closed as of December 2005. We found that timely grant closeout continues to be a significant problem within the Department. Only 13 percent of the 60,933 grants in our sample were closed within 6 months after the grant end date, as required by OJP and OVW policy. We also identified a backlog of over 12,000 expired grants more than 6 months past the grant end date that had not been closed, of which 67 percent had been expired for more than 2 years. In addition, we identified 41 percent of the expired grants that did not comply with grant requirements, including financial and programmatic reporting requirements and local matching fund requirements. We also found that non-compliant grantees had been awarded 129 additional grants totaling $106 million during the period of non-compliance.

We made 44 recommendations that focus on specific steps that the Office of Community Oriented Policing Services (COPS), OJP, and OVW should take to improve the grant closeout process. The components agreed with the majority of our recommendations.

The Department's Efforts to Prevent, Identify, and Recover Improper and Erroneous Payments

Improper payments are payments that should not have been made or payments that were made for an incorrect amount because of errors, poor business practices, or intentional fraud or abuse. According to a February 2006 Office of Management and Budget (OMB) report, *Improving the Accuracy and Integrity of Federal Payments*, the government-wide improper payment total reported for FY 2005 was $37.3 billion.

In recent years, legislation has been enacted requiring government agencies to conduct program inventories and assess each program's risk of making improper payments. The OIG's Audit Division assessed the Department's compliance with legislation pertaining to improper and erroneous payments and evaluated its efforts to prevent, identify, and recover these payments.

Our review examined ATF; DEA; Federal Prison Industries; Justice Management Division (JMD); and the Department's Offices, Boards and Divisions. We found several weaknesses in the components' erroneous payment programs, including that risk assessments did not always include an analysis or review of relevant information such as results from the most recent financial statement audit or data concerning the federal award payments made by recipients and subrecipients. We concluded that identified and recovered improper payment amounts may be understated due to failures in internal controls used to identify and report improper payments. To address these issues, we provided 20 recommendations for improvement to the audited components. The components concurred with each of our recommendations and have begun implementing corrective actions.

Civil Rights and Civil Liberties Complaints

Section 1001 of the *USA Patriot Act* directs the OIG to receive and review complaints of civil rights and civil liberties abuses by Department employees, to publicize how people can contact

the OIG to file a complaint, and to submit a semiannual report to Congress discussing our implementation of these responsibilities. In March 2007, the OIG issued its 10th report summarizing its Section 1001 activities during the period from July 1, 2006, to December 31, 2006.

The report described the number of complaints we received under this section, the cases that were opened for investigation, and the status of these cases. The report also described the status of the recommendations contained in our June 2003 report that reviewed the treatment of aliens held on immigration charges in connection with the investigation of the September 11, 2001, terrorism attacks. In that report, the OIG made 21 recommendations, 20 of which have been resolved. The one open recommendation called for the Department and the DHS to enter into a memorandum of understanding (MOU) to formalize policies, responsibilities, and procedures for managing a national emergency that involves alien detainees. The report noted that, more than 3 years after the OIG made the recommendation and the Department and the DHS agreed to implement it, the MOU has not been signed and the Department and the DHS are still discussing the language of the MOU.

Oversight of Intergovernmental Agreements

The OIG's Audit Division audited the oversight of Intergovernmental Agreements (IGA) within the Department. The IGAs examined in this audit were formal agreements between the USMS and state or local governments to house federal detainees in return for an agreed-upon rate. In FY 2005, the Department spent $750 million, or 75 percent of its $1 billion detention budget, on IGAs. A significant challenge for the Department is to obtain needed detention space for USMS detainees without overpaying for it.

Due to the increase in the number of arrests by federal authorities and the shortage of federally owned detention space, the Department increasingly depends on state and local governments to provide detention space for detainees. Consequently, the USMS, the component responsible for housing and transporting federal detainees from the time they are taken into federal custody until they are acquitted or incarcerated, has about 1,600 IGAs for detention services.

Since 1995, the OIG has audited 31 individual IGAs between the USMS and state and local governments for detention space and questioned almost $60 million in costs from these audits. The OIG found significant deficiencies with how per-inmate costs paid by the Department (known as the "jail-day rates") were established and monitored, including a lack of adequate training for the analysts responsible for negotiating the IGAs and a failure to attempt to recover overpayments from the state and local governments.

However, the Office of the Federal Detention Trustee (OFDT), which manages the Department's detention resource allocations, believes that the audited IGAs were negotiated fixed price agreements and therefore has directed the USMS not to seek reimbursements of the overpayments identified by the OIG. The OIG concluded that OFDT's directive is overbroad and incorrect and recommended that the USMS review each of the audits to determine if repayment or offsets of future payments to the jails are warranted.

In addition, the OIG noted that OFDT is revising its process for entering into IGAs by developing an automated system called eIGA. This system

would allow Department analysts to use statistical models to derive an optimal jail-day rate based on a core rate established using historical IGA rates that are adjusted based on various cost factors. The OIG concluded that while the eIGA system could be a positive step in improving the process, OFDT could significantly improve the new system by expanding the cost information it collects. Using additional cost information will give the USMS more leverage in its negotiations with state and local facilities and help control rising detention costs by reducing negotiated jail-day rates.

The OIG made 10 recommendations to improve the IGA process and ensure that negotiated jail-day rates are fair and reasonable. The USMS agreed with six of our recommendations. The OIG and the Department are discussing how to resolve the remaining recommendations.

The Department's Financial Statement Audits

The *Chief Financial Officers Act of 1990* and the *Government Management Reform Act of 1994* require annual financial statement audits of the Department. The OIG's Audit Division oversees and issues the reports based on the work performed by independent public accountants.

The Department received an unqualified opinion on its FY 2005 and 2006 financial statements. In FY 2006, the Department had one material weakness and one reportable condition, compared to two material weaknesses in FY 2005. The material weakness, which is a repeat from last year, was related to financial management systems general and application controls. The material weakness contained new and continued deficiencies for 8 of the 10 components, including weaknesses in the Department's consolidated information systems general controls environment that provides general control support for several components' financial applications. However, the Department reduced the prior year material weakness on financial reporting to a reportable condition in FY 2006. The reportable condition included several serious but isolated issues, including OJP's grant advance and payable estimation process, ATF's accounts payable process, and the USMS's financial statement quality control and assurance.

We also found improvement at the component level, as evidenced by the reduction in the component material weaknesses from 10 in FY 2005 to 7 in FY 2006. In addition, component reportable conditions dropped from 8 in FY 2005 to 7 in FY 2006. Two components, the DEA and Federal Prison Industries, Inc., continued to have no material weaknesses, reportable conditions, or compliance issues. The table at the end of this discussion compares the FY 2005 and 2006 audit results for the Department's consolidated audit as well as for the 10 individual component audits.

While the Department took a significant step toward reducing its financial material weakness to a reportable condition, it still lacks sufficient automated systems to readily support ongoing accounting operations and financial statement preparation. Many tasks still must be performed manually at interim periods and at the end of the year, requiring extensive efforts on the part of financial and audit personnel. These significant, costly, and time-intensive manual efforts will continue to be necessary until automated, integrated processes and systems are implemented and can readily produce the necessary information throughout the year. While the Department is proceeding toward a Unified Financial Management System that it believes will correct many of these issues, implementation of the system has been slow and will not be completed Department-wide for at least another 6 years.

Comparison of FY 2006 and 2005 Audit Results

Reporting Entity	Auditors' Opinion on Financial Statements		Number of Material Weaknesses: Financial		Number of Material Weaknesses: Information Systems		Number of Reportable Conditions	
	2006	2005	2006	2005	2006	2005	2006	2005
Consolidated Department of Justice	Unqualified	Unqualified	0	1	1	1	1	0
Offices, Boards and Divisions	Unqualified	Unqualified	0	0	0	0	1	1
Assets Forfeiture Fund and Seized Asset Deposit Fund	Unqualified	Unqualified	0	0	0	0	2	1
Federal Bureau of Investigation	Unqualified	Unqualified	0	1	1	1	0	1
Drug Enforcement Administration	Unqualified	Unqualified	0	0	0	0	0	0
Office of Justice Programs	Unqualified	Unqualified	1	2	1	1	1	1
U.S. Marshals Service	Unqualified	Unqualified	1	2	1	1	0	1
Federal Bureau of Prisons	Unqualified	Unqualified	0	0	0	0	1	1
Federal Prison Industries, Inc.	Unqualified	Unqualified	0	0	0	0	0	0
Working Capital Fund	Unqualified	Unqualified	0	0	0	0	2	2
Bureau of Alcohol, Tobacco, Firearms and Explosives	Unqualified	Unqualified	1	1	1	1	0	0
		Component Totals	***3***	***6***	***4***	***4***	***7***	***8***

The Department's Information Security Program Pursuant to FISMA

The *Federal Information Security Management Act* (FISMA) requires the OIG for each federal agency to perform an annual independent evaluation of the agency's information security programs and practices by testing a representative subset of agency systems. OMB has issued guidance to agencies on how to implement policies and practices relating to information security that are compliant with FISMA requirements.

In FY 2006, the OIG's Audit Division audited the security programs of four Department components: the FBI, ATF, DEA, and JMD. Within these components, we reviewed two classified systems – JMD's Cyber Security Assessment and Management (CSAM) Trusted Agent-Secret and the FBI's System Security Information database – and two sensitive but unclassified systems – JMD's CSAM Trusted Agent and ATF's Headquarters Network Infrastructure.

Our review determined that the Department had ensured that all systems within the FBI, ATF, DEA, and JMD were certified and accredited, system security controls were tested and evaluated within the past year, and system contingency plans were tested in accordance with FISMA policy and guidance. However, we found that electronic authentication risk assessments were not performed by the FBI, ATF, or DEA, and the Department's plan of action and milestones process for tracking system vulnerabilities and corrective actions was not fully implemented in accordance with Department policy within the FBI and ATF. Moreover, the Department-wide system configuration policy was not always implemented as required within the DEA and JMD. With respect to IT security awareness training, we found that ATF did not fully ensure that all of its employees were trained as required by Department policy.

As part of the FISMA assessment, we also submitted a response to the Office of the Director of National Intelligence with respect to the FBI's compliance with FISMA requirements for national security systems.

In sum, we provided a total of 31 recommendations for improving the implementation of the Department's information security program and practices for its sensitive but unclassified, classified, and national security systems.

The OIG also evaluated the Department's compliance with OMB guidelines for securing sensitive data to assess whether information security and privacy controls are being developed and implemented. The Department established a task force to develop a comprehensive solution for safeguarding wireless access to personally identifiable information on the Department's internal systems and assess technical solutions to manage remote access to personally identifiable information. Although the Department is in the process of implementing additional security controls to protect personally identifiable information, we found that it is not fully compliant with federal policy for all automated systems currently listed within the Department's IT inventory database. We also found that the Department is not requiring users who access the system remotely to provide two independent ways to authenticate identity, as required by the National Institute of Standards and Technology Special Publications 800-53 and 800-53 A. We provided six recommendations to ensure the Department's compliance with federal policy for securing personally identifiable information. The Department agreed with our recommendations.

Ongoing Work

The Department's Removal of U.S. Attorneys

The OIG and the Department's Office of Professional Responsibility are conducting a joint review of the Department's removal of several U.S. Attorneys. The joint review is examining issues such as whether the removal of any of the U.S. Attorneys was intended to interfere with, or was in retaliation for, either pursuing or failing to purse prosecutions or investigations. In addition, the joint review is examining the accuracy of statements made by various Department officials to Congress about removal of the U.S. Attorneys.

Violent Crime Task Force Coordination

The OIG is reviewing whether investigations conducted by four of the Department's violent crime task forces – ATF's Violent Crime Impact Teams, DEA's Mobile Enforcement Teams, FBI's Safe Streets Task Forces, and USMS's Regional Fugitive Task Forces – are well coordinated. Among other issues, we are examining task force management, cooperation on investigations, deconfliction of events, and information-sharing efforts among the task forces.

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

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

The Department's Victim Notification System

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

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

The OIG is reviewing the procedures that Department components follow to report, identify, and notify affected parties of the loss of sensitive information, including personally identifiable information and classified information. The review also is examining whether components have procedures in place to determine the type of information that was lost.

Inventory of the Department's Major IT Systems

In response to a directive in the Department's FY 2006 Appropriations Act, the OIG is compiling an inventory of all major Department IT systems and planned initiatives and is reporting on all research, plans, studies, and evaluations that the Department has produced, or is in the process of producing, concerning IT systems, needs, plans, and initiatives.

The OIG is issuing three separate reports to address this directive. The first report, issued in March 2006, identified an unverified universe of 46 major Department investments of over $15 million each based on OMB reporting from FY 2005 to projected FY 2007. The second report is collecting cost and other data on major IT systems. The third report is identifying the research, plans, studies, and evaluations related to the Department's IT initiatives and analyzing IT planning problems identified in previous audit reports.

The Department's Key Indicators

The Key Indicators reported each year within the Department's Performance and Accountability Report link to the Department's Strategic Plan and have long-term measurable outcome goals. For each of the Key Indicators, components report on the definition, collection and storage, validation, and limitations of the data. The OIG is auditing Key Indicators for 18 components to ensure that data collection and storage, data validation and verification, and component disclosures regarding data limitation are complete and accurate.

Audit of the Department's Conference Expenditures

In response to a request from the Senate Committee on Appropriations, the OIG is auditing data on costs for selected Department conferences, such as whether the sponsoring component developed a justification for the conferences, conducted cost comparisons on alternative locations to hold the event, and complied with appropriate regulations pertaining to travel and conference expenditures.

Federal Bureau of Investigation

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

Reports Issued

The FBI's Use of National Security Letters

On March 9, 2007, as required by the Patriot Reauthorization Act, the OIG issued a report examining the FBI's use of national security letters (NSL). Under five statutory provisions, the FBI can use NSLs to obtain – without a court order – records such as customer information from telephone companies, Internet service providers, financial institutions, and consumer credit companies. The Patriot Act broadened the FBI's authority to use such letters by lowering the threshold standard for issuing them, allowing the Special Agents in charge of FBI field offices to sign NSLs, and permitting the FBI to use NSLs to obtain full credit reports in international terrorism investigations. The Patriot Reauthorization Act directed the OIG to review the FBI's use and effectiveness of NSLs, including any improper or illegal uses of these authorities.

Our review, which covered the period from 2003 to 2005, found that the FBI's use of NSL authorities has increased in the years since the enactment of the Patriot Act in October 2001. In 2000, the last full year prior to the Patriot Act's passage, the FBI issued approximately 8,500 NSL requests. After the Patriot Act was passed, the FBI dramatically increased its use of NSLs, issuing approximately 39,000 NSL requests in 2003, 56,000 in 2004, and 47,000 in 2005, according to the database the FBI maintains for the purpose of reporting its NSL usage to Congress. In total, during the 3-year period covered by our review, the FBI issued more than 143,000 NSL requests. However, the OIG concluded that these statistics, which were based on information from the FBI's database, significantly understated the total number of NSL requests issued by the FBI because the database was inaccurate and did not include all NSL requests. For example, our examination of case files at 4 FBI field offices found approximately 22 percent more NSL requests in case files we examined than were recorded in the database for those same files.

Our review also examined the effectiveness of NSLs, which are used by the FBI for various purposes, including developing evidence to

support applications for orders issued under the *Foreign Intelligence Surveillance Act* (FISA), developing links between subjects of FBI investigations and other individuals, providing leads and evidence to allow FBI agents to initiate or close investigations, and corroborating information obtained by other investigative techniques. FBI personnel told the OIG that they believe NSLs are indispensable investigative tools in many counterterrorism and counterintelligence investigations.

As directed by Congress, the OIG also examined whether there was any improper or illegal use of NSL authorities. The OIG found that from 2003 to 2005 the FBI identified 26 possible intelligence violations involving its use of NSLs. The possible violations included issuing NSLs without proper authorization, making improper requests under the statutes cited in the NSLs, and conducting unauthorized collection of telephone or Internet e-mail transactional records. In addition to the possible violations reported by the FBI, our review of 77 FBI case files and 293 NSLs in 4 field offices found an additional 22 possible violations. They included improper requests under the pertinent NSL statute and unauthorized collection, due either to FBI or third party error.

The OIG review also identified more than 700 instances in which the FBI improperly obtained telephone toll billing records and subscriber information from 3 telephone companies by issuing "exigent letters" signed by personnel in the FBI's Counterterrorism Division rather than by issuing NSLs. These exigent letters stated they were being issued due to exigent circumstances and the FBI was in the process of obtaining subpoenas for the information. However, the OIG found that the exigent letters were sometimes sent when there was no emergency; that in some instances there were no underlying national security investigations, or documentation of such investigations, tying the exigent letter requests with pending investigations; and that subpoenas had not in fact been submitted to the USAOs' as represented in the letters.

The OIG's review recognized the significant challenges the FBI faced during the period covered by the review and the major organizational changes it was undergoing in that period. Nevertheless, the OIG concluded that the FBI engaged in serious misuse of NSL authorities and in several instances acquired information it was not lawfully authorized to obtain under NSL statutes, such as obtaining consumer full credit reports in counterintelligence investigations.

The OIG made 10 recommendations to the FBI relating to its use of NSLs, including improving its database to ensure that it captures timely, complete, and accurate data on NSLs; issuing additional guidance to field offices to assist in identifying possible intelligence violations arising from the use of NSLs; and taking steps to ensure that it employs NSLs in accordance with the requirements of NSL authorities, Department guidelines, and internal policy. The FBI concurred with all of our recommendations and agreed to implement corrective actions.

The FBI's Use of Section 215 Orders

On March 9, 2007, as required by the Patriot Reauthorization Act, the OIG also issued a report on the FBI's use of Section 215 orders to obtain business records. Section 215 of the Patriot Act allows the FBI to seek an order from the Foreign Intelligence Surveillance Court to obtain "any tangible thing," including books, records, and other items from any business, organization, or entity if the item is for an authorized investigation to protect against international terrorism or clandestine intelligence activity.

Section 215 did not create any new investigative authority but instead significantly expanded

existing authority by broadening the types of records that can be obtained and lowering the evidentiary threshold to obtain an order. Public concerns about the scope of this expanded authority centered on the FBI's ability to obtain library records. However, the OIG review found that the FBI did not obtain Section 215 orders for any library records during the 2002 to 2005 period covered by our review.

Our review found that from 2002 to 2005 the Department, on behalf of the FBI, obtained a total of 21 "pure" Section 215 applications – requests for any tangible item that were not associated with any other FISA authority. In addition, the Department obtained 141 "combination" Section 215 requests that were added to a FISA application for pen register/trap and trace orders to obtain subscriber information.

Our review did not identify any instances involving improper or illegal use of pure Section 215 orders. We found no instance in which the information obtained from a Section 215 order resulted in a major case development, such as disruption of a terrorist plot. We also found that little of the information obtained through Section 215 orders had been disseminated to intelligence agencies outside the Department. However, FBI personnel said they believe the kind of intelligence gathered from Section 215 orders was essential to national security investigations, and the importance of the information was sometimes not known until much later in an investigation – for example, when the information was linked to some other piece of intelligence. FBI officials and Department attorneys stated that Section 215 authority had been useful because it was the only compulsory process for certain kinds of records that could not be obtained through alternative means, such as grand jury subpoenas or NSLs.

The OIG review also found that the FBI had not used Section 215 orders as effectively as it could have because of legal, bureaucratic, or other impediments to obtaining these orders. For example, after passage of the Patriot Act neither the Department nor the FBI issued implementing procedures or guidance on the expansion of Section 215 authority. In addition, we found significant delays within the FBI and the Department in processing requests for Section 215 orders. Finally, we determined through our interviews that FBI field offices did not fully understand Section 215 orders or the process for obtaining them.

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

The OIG's Audit Division issued the second in a series of reports auditing the FBI's ongoing development of its Sentinel IT project, which is intended to upgrade the FBI's case management system and create an automated workflow process.

Our second Sentinel audit found that the FBI has made significant progress in addressing several important areas reported in our first audit of Sentinel, such as: 1) adequately staffing the Sentinel Program Management Office; 2) requiring that Sentinel meet a new joint Department and DHS information sharing standard, which will allow Sentinel to communicate with other systems built to the standard; 3) establishing an Earned Value Management system to monitor Sentinel's project costs and schedule; 4) establishing layers of review, approval, and reporting for Sentinel spending; and 5) completing plans for the independent verification and validation of Sentinel's software to ensure that it will perform as intended.

However, our current audit identified several issues that the FBI must continue to address

as the Sentinel project continues through its first phase of development and enters its more challenging and higher-risk second phase in 2007. We found that the FBI has taken a positive step by establishing a risk management plan that identifies the significant risks associated with the Sentinel project. Yet the contingency plans, and the triggers for activating such plans, exist for only 3 of the 20 identified risks being monitored. With respect to project risks, we viewed the FBI's ability to successfully migrate data from its antiquated Automated Case Support system to Sentinel as a potentially significant challenge. Another significant challenge will be ensuring that Sentinel's software configuration allows all components of the system to work together seamlessly.

The OIG report contained five recommendations that focus on further reducing risks to the Sentinel project, including updating the estimate of total project costs as actual cost data becomes available, developing contingency plans for significant project risks, and filling vacancies in the Sentinel Program Management Office. We will continue to monitor and periodically issue audit reports throughout the four phases of the Sentinel project in an effort to monitor the FBI's progress and identify any emerging concerns.

The FBI's Control Over Weapons and Laptop Computers

The OIG's Audit Division completed a follow-up audit of the FBI's efforts to improve controls over its weapons and laptop computers. The FBI, which maintains more than 52,000 weapons and 26,000 laptops, reported 160 lost or stolen weapons and 160 lost or stolen laptops during a 44-month period from February 2002 through September 2005. This represented a decrease from our prior audit report, issued in 2002, when the FBI reported 354 weapons and 317 laptops lost or stolen during a 28-month period.

While the FBI has made progress in reducing the rate of loss for weapons and laptops, we identified at least 10 of the 160 missing laptops containing sensitive or classified information, 1 of which contained personally identifiable information on FBI personnel. Even more troubling, we found that the FBI could not determine whether 51 additional lost or stolen laptops contained sensitive or classified information. Seven of these 51 laptops were assigned to the Counterintelligence or Counterterrorism Divisions, both of which handle sensitive information related to national security. Without knowing the content of these lost and stolen laptops, it is impossible for the FBI to determine the extent of the damage these losses might have had on its operations or on national security.

Our review also found that, after our 2002 audit, the FBI improved its controls by establishing deadlines for reporting lost and stolen weapons and laptops, entering those losses into the National Crime Information Center (NCIC), and referring the losses for investigation. However, the FBI did not consistently follow these procedures. For example, we found that many of the forms that were used to report both gun and laptop losses were missing critical information such as the date of the loss; whether the loss was entered into NCIC; whether the FBI unit responsible for investigating the loss had been notified; and in the case of laptops, whether they contained sensitive or classified information. We also found that when some of the lost or stolen laptops were identified as containing sensitive or classified information, the FBI examined only a few of those losses to determine the damage they may have had on the FBI's operations and national security.

In addition, our audit determined that the FBI submitted late and inaccurate reports to the Department with respect to losses of its weapons and laptops, did not adequately document its disposal of excess laptops and hard drives to ensure that all sensitive or classified information had been sanitized prior to disposal, and failed

to consistently ensure that departing employees returned their assigned weapons and laptops prior to leaving the FBI.

We made 13 recommendations to the FBI to improve its management controls over weapons and laptops. The FBI agreed with most of our recommendations and outlined a plan for taking corrective action to address all of our recommendations.

The FBI's Response to Congressman Foley's E-mails to a Page

The OIG issued a special report examining the FBI's initial response to e-mails sent by Congressman Mark Foley to a former page with the House of Representatives. The e-mails were forwarded to the FBI in July 2006 by the advocacy group Citizens for Responsibility and Ethics in Washington (CREW). Five of the e-mails were written by Foley to the former page and contained statements that, at a minimum, could be described as unusual between an adult in a position of authority and a juvenile. Three additional e-mails were exchanges between the former page and a House of Representatives employee in which the former page expressed his concern about the nature of Foley's e-mails. Foley resigned from Congress on September 29, 2006, after the e-mails and more explicit instant messages became public.

The OIG found that when the FBI initially received these e-mails, it reviewed them and decided not to investigate them further. This decision was made by an FBI Supervisory Special Agent after consulting with other FBI divisions, including the Crimes Against Children and Adult Obscenity Squad and the Cyber Crimes Squad, mainly because the e-mails were not "sexually explicit" and did not contain "language of persuasion or enticement to engage in any type of activity, criminal or otherwise." We concluded that the Supervisory Special Agent's decision not to open an investigation fell within the range of discretion that she was afforded in her position as a supervisor and did not constitute misconduct.

However, we also determined that the e-mails provided enough troubling indications on their face, particularly given the position of trust and authority that Foley held with respect to pages, that the FBI should have, at the least, taken some follow-up steps, such as interviewing the former page; notifying House of Representatives' authorities in charge of the page program about the concerns expressed by the former page; or sharing its decision to decline the investigation with CREW, who was relying on the FBI to pursue the matter and, as a result, had not notified anyone else about the e-mails.

As part of our review, we also examined inaccurate statements reported in the media attributed to FBI and Department officials when the e-mails became public. In particular, reports that the FBI and the Department stated that CREW had provided heavily redacted e-mails and refused to provide information about the source of the e-mails – which was the reason the FBI did not at the time take further action – were not correct. We attributed these inaccuracies to a misinterpretation of the description of events that was disseminated within the FBI and the Department regarding the FBI's actions in response to the e-mails it received in July.

CODIS Audits

The FBI's Combined DNA Index System (CODIS) includes a national information repository that permits the storing and searching of DNA specimen information to facilitate the exchange of DNA information by law enforcement agencies. During this reporting period, the OIG's Audit Division audited several state and local laboratories that participate in CODIS to determine if they comply with the FBI's Quality

Assurance Standards (QAS) and National DNA Index System (NDIS) requirements. Additionally, we evaluated whether the laboratories' DNA profiles in CODIS databases were complete, accurate, and allowable. Below is an example of our findings:

- The Alabama Department of Forensic Sciences, Birmingham Laboratory in Birmingham, Alabama, was in compliance with standards governing CODIS activities for the areas tested with three exceptions: 1) the Birmingham Laboratory uploaded one potentially unallowable forensic profile into NDIS without receiving a reference sample from the victim because internal controls did not alert the analyst to recognize that the specimen may have originated from a victim, 2) the Birmingham Laboratory did not confirm 2 NDIS offender candidate matches within the required 30 days due to delays caused by the relocation of the lab, and 3) CODIS users did not complete their annual reminder forms for calendar year 2006 at the beginning of the year as required. The Birmingham Laboratory removed the questionable profile from NDIS after identifying the profile in preparation for our audit. We made two recommendations, and the FBI agreed to notify the OIG once the Birmingham Laboratory completed the corrective actions.

Investigations

During this reporting period, the OIG received 852 complaints involving the FBI. The most common allegations made against FBI employees were Intelligence Oversight Board Violations, waste, misuse of government property, and job performance failure. The OIG opened 15 cases and referred other allegations to the FBI's Inspection Division for its review.

At the close of the reporting period, the OIG had 31 open criminal or administrative investigates of alleged misconduct relating to FBI employees. The criminal investigations cover a wide range of offenses, including improper release of information, other official misconduct, and fraud. The administrative investigations involve serious allegations of misconduct. The following are examples of cases involving the FBI that the OIG's Investigations Division handled during this reporting period:

- An investigation by the OIG's Chicago Field Office determined that an FBI Special Agent improperly disclosed a document classified "Secret" and divulged the existence of an FBI search warrant prior to its execution to a female journalism student with whom he had a 2-year extramarital relationship. The investigation also found that the Special Agent engaged in other acts of misconduct, including lying during OIG interviews and in a sworn affidavit, inappropriate use of administrative leave, and violating FBI policy with regard to using his FBI-owned vehicle. The FBI terminated the Special Agent from his position as a result of our investigation.

- An investigation by the OIG's Washington Field Office determined that an FBI Special Agent misused his government-issued travel credit card and undercover credit card by making over $7,500 in personal purchases for phone and utility bills, money transfers, personal travel, electronic goods, clothing, and jewelry. The investigation also found that the Special Agent misused his undercover driver's license. The FBI terminated the Special Agent from his position as a result of our investigation.

- An investigation by the OIG's Washington Field Office led to state charges against an

FBI Special Agent for obstruction of an officer and solicitation of prostitution. In lieu of prosecution, the Special Agent entered into an agreement with a West Virginia State special prosecutor acknowledging that he had inappropriate sexual relations with a convicted prostitute in an FBI vehicle while he was on duty and that he had inappropriately approached local law enforcement regarding dismissal of pending criminal charges against the prostitute. As part of the agreement, the Special Agent resigned from his position with the FBI and agreed not to seek or accept in the future any position with a department or agency of the U.S. government or any law enforcement agency.

- In our September 2006 *Semiannual Report to Congress*, we reported on a case in which an investigation by the OIG's Dallas Field Office led to the conviction of an FBI Special Agent in Charge (SAC) on charges of making false statements. The jury found that the SAC concealed material facts from the FBI concerning his relationship and financial dealings with a Mexican national who had alleged Mexico drug cartel associations and was a former confidential informant. The SAC also made false statements on his 2002 Public Financial Disclosure Report regarding gifts he received from the former confidential informant. During this reporting period, the SAC was sentenced to 6 months' incarceration and 3 years' supervised release and ordered to pay a $10,000 fine and perform 200 hours of community service.

- In our September 2006 *Semiannual Report to Congress*, we reported on an investigation by the OIG's Los Angeles Field Office, which determined that an FBI Special Agent frequented an adult entertainment club in Las Vegas and accepted monetary, sexual, and other gratuities from the club owner over a 6-year period. The investigation also determined that the Special Agent allowed the club owner to use his FBI vehicle on at least two occasions and provided the owner with sensitive law enforcement information. During this reporting period, the FBI terminated the Special Agent from his position as a result of our investigation.

Ongoing Work

The FBI's Use of National Security Letters in 2006

As required by the Patriot Reauthorization Act, the OIG is continuing to review the FBI's use of NSLs in 2006. We also are monitoring the FBI's corrective action taken in response to our March 2007 report regarding the use of these authorities in prior calendar years.

The FBI's Use of Section 215 Orders in 2006

As required by the Patriot Reauthorization Act, the OIG is continuing to review the FBI's use of Section 215 orders in 2006 to obtain business records.

Sentinel: Status of the FBI's Case Management System

The OIG is conducting its third audit in a series of reports examining the FBI's ongoing development of its Sentinel case management project. Our third audit of Sentinel is assessing the overall status of the Sentinel project and

whether the first two phases of the project are meeting budget, schedule, and performance expectations. We also are evaluating whether the FBI's management controls and provisions of the Sentinel contract provide reasonable assurance that it will be completed successfully and efficiently, and determining the status of the FBI's efforts to resolve the concerns discussed in our previous reports.

FBI Reports of Alleged Abuse of Military Detainees

The OIG is reviewing FBI employees' observations and actions regarding alleged abuse of detainees at Guantanamo Bay, Abu Ghraib prison, and other venues controlled by the U.S. military. The OIG is examining whether FBI employees participated in any incident of detainee abuse, whether FBI employees witnessed incidents of abuse, whether FBI employees reported any abuse, and how those reports were handled by the FBI. In addition, the OIG is assessing whether the FBI inappropriately retaliated against or took any other inappropriate action against any FBI employee who reported any incident of abuse.

Follow-up Examining Hanssen Review Recommendations

The OIG is completing its follow-up review of the FBI's progress in implementing recommendations contained in our August 2003 report entitled, "A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen." Our previous report made 21 recommendations to help the FBI improve its internal security and enhance its ability to deter and detect espionage. The Hanssen follow-up review is assessing the FBI's response to recommendations in the report.

Follow-up Review of the Terrorist Screening Center

A June 2005 OIG audit report assessed the Terrorist Screening Center's consolidated terrorist watch list database and computer systems, as well as staffing, training, and oversight of the Call Center. In this follow-up review, we are auditing the Center's efforts to ensure the quality of the information in the watch list database and its attempts to minimize the impact for individuals incorrectly identified as watch list subjects.

The FBI's Efforts to Combat Crimes Against Children

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

The FBI's Progress in Hiring, Training, and Retaining Intelligence Analysts

The OIG issued a report in May 2005 examining the FBI's efforts to hire, train, and retain intelligence analysts. This follow-up audit examines the FBI's continuing efforts to develop its intelligence analyst corps and the FBI's progress in implementing the recommendations we made in our prior audit.

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

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

Drug Enforcement Administration

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

Reports Issued

The DEA's International Operations

Since 2003, the DEA has increased the number of its foreign offices, bolstered its international funding, and augmented the number of personnel assigned to combat foreign drug trafficking and organizations. The OIG's Audit Division reviewed the DEA's international operations and concluded that the DEA has established valuable relationships with its foreign counterparts that assist its efforts to combat major drug trafficking organizations that affect the United States. DEA performance data indicates that its international offices are pursuing high-priority cases and have succeeded in disrupting and dismantling many drug trafficking organizations. In addition, we found that the DEA's international partners speak positively about the DEA's training of foreign law enforcement personnel.

Our audit also found that certain aspects of the DEA's international operations could be improved. For example, the DEA does not have a standardized system to track leads and requests for assistance received by its foreign offices. Without such a system, the DEA could not objectively assess the quantity or quality of support that its foreign offices provided to other DEA offices and law enforcement agencies.

Our audit also revealed deficiencies with the DEA's management and oversight of its Vetted Unit Program, an initiative that involves screening and training foreign law enforcement personnel and funding them to perform work on behalf of the DEA. The deficiencies included poor record keeping, inadequate practices for paying foreign personnel who participate in the Vetted Unit Program, exceeding the recommended ratio of DEA advisors assigned to monitor the program compared to the number of foreign personnel participating in the program, insufficient evidence of training, and failure to perform exit briefings of outgoing foreign personnel leaving the program.

The OIG made 22 recommendations to assist the DEA in improving the management and operation of its international activities. The DEA agreed with the majority of our recommendations and outlined a plan for corrective action.

The DEA's Handling of Cash Seizures

From October 1, 2003, to November 3, 2005, the DEA made 16,007 cash seizures totaling nearly $616 million. Cash seized by the DEA is eventually transferred to the USMS for safekeeping until it is either forfeited by or returned to its owner. The OIG's Audit Division audited the DEA's handling of cash that it seizes during the course of its investigations.

Our audit determined that the DEA has internal control policies for handling and safeguarding seized cash, such as requiring that a witness be present at critical stages of the cash handling process, counting the seized cash immediately unless the amount of cash seized makes an immediate count impracticable, and completing documentation detailing the disposition of the seized cash. However, the DEA failed to consistently follow or document compliance with these policies.

For example, we often found no documentation indicating whether a witnessing agent or task force officer was present at critical stages of the cash handling process, as required by DEA policy. We also identified many instances where agents and task force officers failed to count the seized cash; provide a receipt to the subject from whom the cash was taken; complete documents transferring custody of the cash to an evidence custodian; or record the receipt, transfer, or disposal of the cash in a temporary or permanent control ledger.

Failure to follow DEA policies on counting seized cash can lead to various problems, including allegations of theft against DEA agents. Our review of 33 internal DEA investigations involving allegations that DEA agents had either lost or stolen defendants' property found that in 11 instances DEA agents did not properly handle, process, or dispose of the evidence. Some of the cases involved multiple violations of DEA policies.

The OIG made seven recommendations to improve the DEA's handling of seized cash. The DEA agreed with all but one of our recommendations.

Investigations

During this reporting period, the OIG received 210 complaints involving the DEA. The most common allegations made against DEA employees included job performance failure, theft, waste, and mismanagement. The OIG opened 9 investigations and referred other allegations to the DEA's Office of Professional Responsibility for review.

At the close of the reporting period, the OIG had 16 open cases of alleged misconduct against DEA employees. The most common allegations were theft and improper release of information. The following are examples of cases involving the DEA that the OIG's Investigations Division investigated during this reporting period:

- An investigation by the OIG's Denver Field Office determined that a DEA Special Agent fraudulently obtained a government-funded permanent change of duty station transfer by falsely claiming that his wife suffered from cancer. The DEA had expended $47,805 to relocate the Special Agent and his family. The USAO for the District of Wyoming has filed a civil *False Claims Act* complaint in the District of Utah seeking repayment of funds and damages from the Special Agent.

- A joint investigation by the OIG's Los Angeles Field Office and the DEA's Office of Professional Responsibility led to the arrest of a DEA contracting officer on charges of corruptly profiting from his employment as a federal agent and making a false statement. The joint investigation developed evidence that the contracting officer received for his personal use

21 checks totaling $13,442 from a DEA vendor whose contract he managed. The contracting officer also failed to disclose on his financial disclosure form the funds he received from the vendor. Judicial proceedings continue.

Ongoing Work

The DEA's Control Over Weapons and Laptop Computers

In August 2002, the OIG issued a report auditing the DEA's internal controls over its weapons and laptop computers that detailed significant lapses in the control over management of these assets. This follow-up audit is examining the effectiveness of DEA's current initiatives to manage these critical assets and determine if the DEA has taken corrective action on the recommendations in the original audit report.

The DEA's Utilization of Intelligence Analysts and Reports Officers

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

Office of Justice Programs

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

Reports Issued

Cooperation of SCAAP Recipients in the Removal of Criminal Aliens

As required by Congress, the OIG audited whether states and localities that receive OJP funding under the State Criminal Alien Assistance Program (SCAAP) have fully cooperated with the DHS's Immigration and Customs Enforcement (ICE) in its effort to remove criminal aliens from the United States. SCAAP provides federal assistance to states and localities for the costs of incarcerating certain criminal aliens who are in custody based on state or local charges or convictions. In FY 2005, OJP distributed $287 million to 752 jurisdictions under SCAAP. Our audit did not disclose any instances of failure by SCAAP recipients to cooperate with ICE in the removal of criminal aliens from the United States.

Congress also directed the OIG to report on the number of criminal offenses committed by aliens unlawfully present in the United States after being apprehended by state or local law enforcement officials for a criminal offense and subsequently released without referral to ICE for removal from the United States, including aliens who were released because the state or local entity lacked space or funds for detention. The OIG sampled the criminal histories of 100 aliens who were included in SCAAP applications for FY 2004 funding. We found that 73 of the 100 individuals had more than 1 arrest.

Based on the information available to us in the criminal histories, we could not determine the number of criminal aliens in our sample who were deported and later arrested after reentering the United States. Moreover, based on our limited sample, the OIG could not statistically extrapolate the number of offenses committed by all criminal aliens who were released from local custody by SCAAP recipients without a referral to ICE. However, if this data is indicative of the full population, the rate at which released criminal aliens are rearrested is extremely high.

The National Court-Appointed Special Advocate Program

Since 1993, OJP has provided grants totaling $100 million to the National Court-Appointed

Special Advocate Association (NCASAA), which provides funding for court-appointed special advocate (CASA) programs. The purpose of the CASA program is to ensure that abused and neglected children receive high-quality, sensitive, effective, and timely representation in court hearings to determine their guardianship.

As required by Congress, the OIG audited NCASAA to determine the types of activities NCASAA has funded and the outcomes in cases where CASA volunteers were involved compared to cases where CASA volunteers were not involved. Based on the available data, we found that in cases where CASA volunteers were involved:

- the children spent more time in foster care;
- the children and their parents were ordered by the courts to participate in more services and received more services;
- the children were less likely to reenter the Child Welfare System; and
- the children were more likely to be adopted and less likely to be reunified with their parents.

Although the outcomes for cases involving a CASA volunteer appear to be less favorable in some instances than cases not involving a CASA volunteer, this may be a result of the fact that cases involving a CASA volunteer are typically the most serious cases of maltreatment.

We found that OJP established outcome measures for its CASA grant programs but these measures did not address the effectiveness of the programs in meeting the needs of children in the Child Welfare System. Additionally, none of the outcome measures established by OJP addressed the outcome measures mandated for this audit.

We made two recommendations that focus on steps OJP should take to improve the CASA grant program. OJP agreed with both recommendations.

National Law Enforcement and Corrections Technology Centers

The National Law Enforcement and Corrections Technology Centers (NLECTC) program was established in 1994 to provide a mechanism for facilitating the introduction of new technologies into the law enforcement community and to provide technical assistance to state and local law enforcement in implementing those technologies. NLECTC is managed by NIJ and comprised of 10 centers located throughout the country. In FYs 2004 and 2005, Congress allocated $33.3 million and $30.2 million, respectively, to NIJ to fund NLECTC operations.

The OIG's Audit Division tested the NLECTC program's accounting records by sampling $2.6 million in expenditures for personnel, travel, consultants, contractors, other direct costs, and indirect costs. Our test results identified several weaknesses, including $472,069 in grant-related expenditures that were not adequately supported. In addition, we identified $224,936 in unallowable expenditures, most of which resulted from an over-billing of indirect costs to the Rural Law Enforcement Technology Center in Hazard, Kentucky. We also identified a potential conflict of interest at the NLECTC-Rocky Mountain operation in Denver, Colorado, where several employees had private businesses that offered the same products and services that they, as NLECTC employees, were responsible for as advisers to local law enforcement.

We provided three recommendations to address the weaknesses identified in this audit. OJP agreed with our recommendations.

OJP Grants to State and Local Entities

During this reporting period, the OIG continued to audit grants awarded by OJP. Examples of findings from OIG audits issued during this period include the following:

- OJP awarded a $249,352 Identity Theft Verification/Passport cooperative agreement to the Ohio Attorney General's Office, Crime Victims Services Section (CVSS) to assist in its efforts to provide victims of identity theft with a means of demonstrating to law enforcement and creditors that their identity has been stolen. Our audit found that CVSS's controls over federally reimbursed expenditures were adequate to ensure that such expenses were properly accounted for and that transactions were accurately recorded and supported. However, we found that CVSS could not support its required match of $154,657 for salary, fringe benefit, and supply costs. As a result, we questioned the total local matching costs and made four recommendations. OJP agreed with all of our recommendations.

- NIJ provided a $525,815 Solving Cold Cases with DNA grant to the City of North Miami, Florida, to assist in its efforts to apply new DNA technologies to solve 22 homicide and 300 sex crime cases. Our audit determined that North Miami was accomplishing the required performance and generally complied with grant requirements. However, we found that North Miami did not maintain an accurate and timely method for reconciling grant payments to its accounting records and had mistakenly drawn down $86,020 from the fund due to an error in the automated system at OJP. We also found that North Miami had drawn down $130,352 in excess of actual expenditures as an advance of 1 year's budgeted grant expenditures. Subsequent to the conclusion of our audit field work, North Miami took corrective action to reimburse OJP the $86,020 drawn down in error and the $130,352 drawn down in excess of actual expenditures. North Miami also took actions to correct flaws in its general ledger system. Consequently, we made no recommendations.

- OJP awarded a $49.9 million grant to the City of New York Police Department (NYPD) to provide traffic control, counterterrorism intelligence, and physical security to delegates, visitors, and venues at the 2004 Republican National Convention. We determined that the NYPD generally complied with grant requirements in the areas we tested. However, the NYPD only submitted two of the five required progress reports and submitted those two reports significantly late. In addition, NYPD never submitted six of the nine required Financial Status Reports, did not maintain adequate documentation for all grant expenditures, and made errors in calculating some expenditures. The NYPD also could not provide sufficient documentation for 30 of the 408 sample employees we tested whose payroll expenditures were charged to the grant, and we found that some of the charges were unallowable. Our report contained three recommendations. OJP agreed with the recommendations.

The National Procurement Task Force

During this reporting period, the Department organized the National Procurement Fraud Task Force, which is designed to coordinate the efforts of the Department and the federal Inspectors General in promoting the prevention, detection, and prosecution of procurement fraud, including grant fraud. The mission of the Task Force is to focus federal efforts on procurement fraud, such as

defective pricing, product substitution, misuse of classified and procurement sensitive information, false claims, labor mischarging, grant fraud, ethics and conflict of interest violations, and public corruption associated with procurement and grant fraud.

The OIG is chairing the Grant Fraud Committee of the Task Force, which focuses on the fraud issues that the federal government faces in awarding and overseeing grants. The Grant Fraud Committee is focusing on three areas: 1) enhancing information sharing concerning grant fraud; 2) coordinating efforts to provide training to auditors, agents, and prosecutors on detecting, investigating, and prosecuting grant fraud; and 3) conducting outreach to agency program managers and to communicate best practices on deterring and investigating grant fraud.

Investigations

During this reporting period, the OIG received 10 complaints involving OJP. The most common allegation made against OJP employees, contractors, or grantees was grantee fraud. The OIG opened two investigations and referred other allegations to OJP management for review.

At the close of the reporting period, the OIG had 17 open cases of alleged misconduct against OJP employees, contractors, or grantees. The following are examples of cases involving OJP that the OIG's Investigations Division investigated during this reporting period:

- A joint investigation by the OIG's Chicago Field Office and the Chicago Regional Audit Office led to the arrest, guilty plea, and sentencing of the Executive Director of the Chicago-based nonprofit organization National Training and Information Center for theft of federal program funds. The investigation determined that the Executive Director intentionally misused OJP Technical Assistance Grants to lobby Congress for additional grant funds. The Executive Director was sentenced to 5 months' incarceration, 5 months' home confinement, and 24 months' supervised release. He also was fined $5,000 and ordered to pay $46,528 in restitution. A civil *False Claims Act* action against the National Training and Information Center seeking $207,131 in damages continues.

- A joint investigation by the OIG's San Francisco Area Investigations and Audit Offices, along with the FBI, Department of Housing and Urban Development (HUD), and Internal Revenue Service (IRS) led to the arrest of the former Mayor of Fairbanks, Alaska, and his wife pursuant to a 92-count indictment charging them with theft of $450,000 in federal grant funds, conspiracy, and money laundering. The investigation developed evidence that the former Mayor and his wife misappropriated federal grant funds from OJP and HUD that were designated to operate a non-profit organization called Love Social Services Center. Instead they used the funds for personal use and to partially fund the building of their church. A trial is pending.

- A joint investigation by the OIG's Fraud Detection Office and Boston Area Office, along with the FBI, IRS's Criminal Investigations Division, and Massachusetts State officials led to allegations that a former Director of Programs at the Massachusetts Executive Office of Public Safety violated state ethics laws by negotiating employment with a company while simultaneously awarding OJP grant funds to clients of that company. The Massachusetts State Ethics Commission filed an Order to Show Cause advising that the Commission will take disciplinary measures against the former Director of Programs unless he provides justification for his actions.

The Order to Show Cause alleges that the former Director of Programs negotiated employment with a public safety consulting firm while at the same time approved nearly $1.12 million in OJP grant payments to clients of the firm. The investigation found that during his tenure as Director of Programs, he made numerous decisions affecting the award of over $10 million in OJP grant funds and directed a large portion of the funds to police departments that had a relationship with the consulting firm, which earned approximately $2 million in fees for securing these grant funds. After the Director of Programs resigned from his position with the Commonwealth of Massachusetts he accepted a position with the consulting firm.

- An investigation by the OIG's Fraud Detection Office led to the arrest and guilty plea of a civilian for theft of government program funds. The investigation found that the comptroller for the American Prosecutors Research Institute embezzled $76,464 in OJP grant funds. The comptroller accessed the grant funds by writing checks to herself and using an unauthorized debit card over the course of several years. Sentencing is pending.

Ongoing Work

Forensic Science Grants

The OIG is conducting a follow-up to its review of OJP's Paul Coverdell Forensic Science Improvement Grant Program, which is intended to assist state and local governments in eliminating backlogs in analyzing forensic evidence and improve the quality and reliability of forensic laboratory results. The OIG is reviewing OJP's administration of the requirement for grantees to certify that "a government entity exists and an appropriate process is in place to conduct independent external investigations into allegations of serious negligence or misconduct" against forensic laboratories that receive Coverdell grant funds.

Management of the Grant Program for Human Trafficking Victims

The *2000 Trafficking Victims Protection Act* enables OVC to support the development or enhancement of victim service programs for alien victims trafficked into or within the United States who require emergency services. The OIG audit is determining the extent to which the grant program has achieved its objective to provide effective assistance for victims of trafficking.

U.S. Marshals Service

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

Reports Issued

The USMS's Management of the Justice Prisoner and Alien Transportation System

The OIG's Audit Division audited the Justice Prisoner and Alien Transportation System (JPATS), a USMS program that provides air transport of prisoners and aliens in federal custody within the continental United States, Central America, and the Caribbean. We found several deficiencies in JPATS, including a lack of planning to predict future capacity needs, a failure to reduce costs by maximizing the number of passengers scheduled for each flight, and inadequate mechanisms to ensure that certain safety procedures are followed.

Despite the fact that the overall demand for prisoner and alien transportation has grown over the past 6 years, our audit found that JPATS has not yet developed a planning tool that allows it to project prisoner and alien movements more than 1 year into the future. This lack of capacity planning has led to underutilization of available seats on JPATS aircraft because JPATS has not amended its flight schedules to maintain a more optimal use of its resources. For example, in our review of flight data from 1,034 flights between FY 2004 and the first quarter of FY 2006, we found that 74 percent of the seats were filled on flights originating from one of the three hubs reviewed, but less than half of the seats were filled on flights originating from the two remaining hubs. In addition, we found that JPATS has been using short-term leases for its large aircraft since early 2005 despite studies by the Government Accountability Office and OFDT that found cost savings could be realized either by purchasing the aircraft or entering into long-term leases.

While our audit noted that JPATS has developed adequate internal policies to ensure that it conducts its air transportation in a safe and secure manner, we found that JPATS generally does not have the necessary systems in place to adhere to its own standards on safety and security. For example, we found 57 instances where JPATS crew members did not appear to have received the

entitled rest prescribed by JPATS policy. We also found that improvements were needed to ensure that JPATS met its objectives in security staffing.

Our report contained 15 recommendations for USMS to develop capacity planning tools; replace the current, expensive short-term aircraft leases with long-term options; and develop mechanisms to ensure that JPATS safety and security policies are followed. The USMS agreed with all of our recommendations and is in the process of implementing them.

Investigations

During this reporting period, the OIG received 212 complaints involving the USMS. The most common allegations made against USMS employees included job performance failure and other official misconduct, misuse of a credit card, and use of unnecessary force. The OIG opened 7 investigations and referred other allegations to the USMS's Office of Internal Affairs for review.

At the close of the reporting period, the OIG had 16 open cases of alleged misconduct against USMS employees. The following is an example of a case involving the USMS that the OIG's Investigations Division investigated during this reporting period:

- The OIG's Chicago Field Office investigated allegations that a U.S. Marshal allegedly used USMS funds to pay overtime and buy gifts for a USMS contract guard who allegedly was his girlfriend or wife. The OIG investigation did not develop evidence to substantiate these allegations, but found that the U.S. Marshal was responsible for the hiring of the USMS contract guard and had a personal and financial relationship with her that constituted a conflict of interest. The case was declined for prosecution, and the OIG referred the case to the USMS for appropriate action.

Ongoing Work

Judicial Security

The OIG is reviewing the USMS's efforts to protect the federal judiciary. This is a follow-up to our 2004 inspection of the USMS's efforts since September 11, 2001, to improve its protection of the federal judiciary, focusing specifically on the USMS's ability to assess reported threats against the judiciary, collect and analyze intelligence to identify potential threats against the judiciary, and determine appropriate measures to protect members of the federal judiciary during high-threat trials and while they are away from the courthouse. The follow-up review also examines the USMS's efforts to implement preventive measures such as home alarms to protect federal judges.

The USMS's Workforce Composition

The OIG is auditing how the USMS's management of its human resources is affecting its organizational performance. Specifically, we are examining the USMS's workforce planning efforts and reviewing spending, utilization, and program data to determine whether resources are used efficiently and effectively to achieve organizational objectives. We also are assessing whether the USMS is providing adequate and appropriate training to its employees.

Federal Bureau of Prisons

The BOP operates a nationwide system of prisons and detention facilities to incarcerate those imprisoned for federal crimes and detain those awaiting trial or sentencing in federal court. The BOP has approximately 36,000 employees and operates 114 institutions, 6 regional offices, and 2 staff training centers. The BOP is responsible for the custody and care of approximately 192,000 federal offenders, 162,000 of whom are confined in BOP-operated correctional institutions and detention centers. The remainder are confined in facilities operated by state or local governments or in privately operated facilities.

Investigations

During this reporting period, the OIG received 2,765 complaints involving the BOP. The most common allegations made against BOP employees included job performance failure and other official misconduct and force, abuse, and rights violations. The vast majority of complaints dealt with non-criminal issues that the OIG referred to the BOP's Office of Internal Affairs for review.

At the close of the reporting period, the OIG had 254 open cases of alleged misconduct against BOP employees. The criminal investigations cover a wide range of allegations, including introduction of contraband into BOP facilities, bribery, and sexual abuse. The following are examples of cases involving the BOP that the OIG's Investigations Division handled during this reporting period:

- In our September 2006 *Semiannual Report to Congress* we reported on a case in which a joint investigation by the OIG's Miami Field Office and the FBI led to the indictment of six BOP correctional officers assigned to the Federal Correctional Institution (FCI) in Tallahassee, Florida, on charges of conspiracy to sexually abuse female inmates and introduction of contraband. The investigation determined that the correctional officers were involved in a scheme to provide contraband to the female inmates in exchange for sexual favors and money. In a joint operation to arrest the defendants, one of the indicted correctional officers began firing. He hit and killed OIG Special Agent William "Buddy" Sentner III. However, before he died, Special Agent Sentner courageously returned fire, killing the correctional officer before he could shoot others.

  During this reporting period, two of the six correctional officers were sentenced; the first received 12 months' incarceration followed by 3 years' supervised release, and the second received probation. Two other correctional officers were convicted at trial on charges of bribery and witness tampering. One was

sentenced to 12 months' incarceration and 3 years' supervised release and fined $6,000, while the other was sentenced to 12 months' incarceration and 3 years' supervised release and fined $3,000. The fifth correctional officer pled guilty to conspiracy charges and was sentenced to 36 months' probation and 12 months' home confinement. The sixth correctional officer was the one killed in the exchange of gunfire that he initiated.

- A joint investigation by the OIG's San Francisco Area Office and the DEA resulted in the arrest, conviction, and sentencing of a BOP correctional officer assigned to the U.S. Penitentiary in Atwater, California. During an undercover operation, the correctional officer accepted 5 ounces of black tar heroin and a $5,000 bribe to smuggle the heroin into the penitentiary. He was sentenced to 37 months' incarceration and 36 months' supervised release pursuant to his guilty plea to a charge of possession of heroin with intent to distribute.

- An investigation by the OIG's New York Field Office developed evidence that a BOP laundry foreman accepted $6,200 in cash to smuggle cellular phones and controlled substances into the FCI in Fort Dix, New Jersey. The laundry foreman was sentenced to 30 months' incarceration and 36 months' supervised release for accepting bribes to introduce contraband into the prison.

- An investigation by the OIG's Dallas Field Office led to the arrest of a BOP inmate housed at the Dismas Charities Community Corrections Center in Midland, Texas. The inmate was indicted for making a false statement to a government agency. The investigation determined that the inmate falsely claimed to the OIG that she was sexually assaulted by a male resident monitor at the corrections center. When confronted by OIG investigators, the inmate admitted she was not sexually assaulted. The resident monitor was exonerated.

- An investigation by the OIG's Atlanta Area Office led to the arrest and guilty plea of two BOP contract correctional officers assigned to the Rivers Correctional Institution (RCI) in Winton, North Carolina, for falsifying an official report to influence a federal investigation. The OIG investigation developed evidence that the correctional officers conspired with an RCI inmate to plant a knife in the property of another inmate whom the correctional officers thought was spreading rumors about the correctional officers' sexual relations with two inmates. As a result, the second inmate's parole release date was delayed 9 months. The correctional officer who planted the knife and falsely claimed to have found the knife during a subsequent search of the inmate's cell also falsified a BOP Incident Report describing the seizure, which the U.S. Parole Commission relied upon to delay the inmate's parole date. Sentencing is pending for both correctional officers.

- An investigation by the OIG's Dallas Field Office led to the arrest and guilty plea of a BOP inmate systems manager assigned to the Federal Prison Camp in Bryan, Texas, on charges of sexual abuse of a ward, abusive sexual contact with a ward, and providing false statements. The investigation identified five female inmates with whom the inmate systems manager sexually abused while working at the prison camp. The inmate systems manager resigned from his position as a result of this investigation. Sentencing is pending.

Ongoing Work

The BOP's Efforts to Manage Inmate Health Care

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

The BOP's Administration of the Witness Security Program

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

Review of Health and Safety Issues at BOP Computer Recycling Facilities

The OIG is investigating allegations that the BOP failed to adequately address allegations that workers and inmates at several BOP institutions were exposed to unsafe levels of lead, cadmium, and other hazardous materials in computer recycling plants operated by Federal Prison Industries, Inc. (UNICOR). The OIG initiated this investigation after the Office of Special Counsel concluded that an earlier investigation by the BOP failed to adequately address allegations by a BOP safety manager that UNICOR's computer recycling operations were unsafe.

U.S. Attorneys' Offices

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

Reports Issued

Critical Incident Response Plans

During this reporting period the OIG issued a follow-up report to our 2003 review of USAOs' Critical Incident Response Plans. Each USAO is responsible for developing its Critical Incident Response Plan to respond quickly and appropriately to critical incidents, including acts of terrorism, hostage situations, and natural disasters. Our 2003 review found that a model plan the Department prepared for USAOs to follow while implementing their own response plans was deficient in several aspects, and that USAOs generally did not follow the standard practice of conducting regular critical incident response exercises.

Our current review found that, while USAOs, EOUSA, and the Department's Counterterrorism Section (CTS) had taken important steps to improve USAOs' preparedness, most USAOs have since regressed in their required Critical Incident Response Plan activities, and EOUSA and CTS are not providing USAOs with necessary direction and support.

Since our 2003 review, the Department revised its model plan to address the OIG's recommendations. All 93 USAOs had conducted at least one critical incident preparation exercise and completed an after-action report, and 53 had conducted 2 or more exercises between May 2004 and November 2006. In addition, we found that the Department has provided improved training and guidance to USAOs' Crisis Management Coordinators, who are the designated persons in each district responsible for implementing and overseeing their district's response plan.

In this follow-up review, USAOs from the Gulf Coast reported that conducting critical incident response exercises proved invaluable in producing timely decision making by managers during the hurricanes in 2004 and 2005. However, we also found that many USAOs have regressed in some of their required Critical Incident Response Plan activities. For example, contrary to the revised guidelines, many USAOs have not continued to conduct critical incident response exercises on an annual basis or continued to complete after-action reports after conducting exercises.

The OIG made seven recommendations to help the Department continue to improve USAOs' ability to respond quickly and appropriately to critical incidents. The Department concurred with all of the recommendations.

Investigations

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

- An investigation by the OIG's Tucson Area Office resulted in the resignation of an Assistant U.S. Attorney (AUSA). The investigation determined that the AUSA, while representing the Department at a training seminar, groped and made unwanted sexual advances toward a female trainer. During his interviews with OIG investigators, the AUSA provided conflicting statements regarding his interaction with the woman. When confronted about his conflicting statements, the AUSA resigned in lieu of prosecution.

Other Department Components

Criminal Division

Reports Issued

Equitable Sharing Audits

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

During this reporting period, the OIG's Audit Division audited the Iowa Department of Public Safety (Iowa DPS) to assess whether equitable sharing assets were accounted for properly and used for allowable purposes as defined by the applicable regulations and guidelines. We found that the Iowa DPS generally complied with equitable sharing guidelines. However, we found weaknesses related to its Federal Annual Certification Reports, tracking and reconciliation of sharing requests, and the use of equitable sharing revenues. Specifically, we found that the Iowa DPS did not track equitable sharing requests and receipts, and receipts were not deposited in a timely manner. We also found that the Iowa DPS did not use equipment purchases totaling $53,150 for law enforcement purposes and could not provide adequate supporting documentation for expenditures totaling $536,820. As a result, we made 4 recommendations to strengthen the Iowa DPS's receipt tracking and deposit procedures as well as request support for the budget section of its FY 2004 and 2005 Annual Certification Reports and to remedy $589,970 in unsupported and unallowable expenditures totaling approximately 19 percent of the total grant funds. The four recommendations are open and resolved.

Bureau of Alcohol, Tobacco, Firearms and Explosives

Ongoing Work

National Firearms Registration and Transfer Record

The OIG is reviewing ATF's National Firearms Registration and Transfer Record to determine whether ATF has effective policies and procedures to reliably maintain records of registrations and transfers of *National Firearms Act* weapons.

Gun Shows

The OIG is reviewing ATF's enforcement policies and practices related to firearms trafficking at gun shows. The review will provide information about ATF's presence at gun shows and the policies, procedures, and oversight mechanisms that guide ATF's activities.

Office of Community Oriented Policing Services

Investigations

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

- An investigation by the OIG's Fraud Detection Office resulted in the City of Hazlehurst, Georgia, paying restitution in the amount of $177,109 to COPS for misapplication of grant funds. The city police department applied for COPS funds in the amount of $216,000 to hire 2 officers for a 3-year deployment to their school resource program. The officers were required to attend specialized training and be deployed full-time to elementary, middle, and high schools. The investigation disclosed that the police chief only deployed 1 untrained officer to the schools for a 1-year period. Two other officers were hired with the grant funds but were assigned regular patrol shifts. The matter was declined for prosecution in lieu of the administrative recovery.

Executive Office for U.S. Trustees

Ongoing Work

Monitoring and Oversight of Chapter 7 Panel Trustees

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

Top Management and Performance Challenges

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

The OIG's current list of top challenges, issued in October 2006, is to the right. The challenges are not presented in order of priority – we believe that all are critical management and performance issues facing the Department. However, it is clear that the top challenge facing the Department is its ongoing response to the threat of terrorism. Several other top challenges are closely related to and impact directly on the Department's counterterrorism efforts.

Many of the challenges from last year's list remain and are long-standing, difficult challenges that will not be solved quickly or easily. However, we removed the challenges of "Department and FBI Intelligence-Related Reorganizations" and "Judicial Security" from the 2005 list, combined "Information Technology Security" with "Information Technology Systems Planning and Implementation," and added the challenges of "Cybercrime," "Violent Crime," and "Civil Rights and Civil Liberties."

Top Management and Performance Challenges in the Department of Justice – 2006

1. Counterterrorism
2. Sharing of Intelligence and Law Enforcement Information
3. Information Technology Planning, Implementation, and Security
4. Violent Crime
5. Financial Management and Systems
6. Detention and Incarceration
7. Supply and Demand for Drugs
8. Grant Management
9. Civil Rights and Civil Liberties
10. Cybercrime

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

Congressional Testimony

On March 28, 2007, the Inspector General testified before the House Permanent Select Committee on Intelligence on the OIG's review of the FBI's use of national security letters and the FBI's use of Section 215 orders to obtain business records.

Similarly, on March 21, 2007, the Inspector General testified before the Senate Judiciary Committee and on March 20 testified before the House Judiciary Committee on the OIG's review of the FBI's use of national security letters and Section 215 orders for business records.

On March 22, the Inspector General and OIG staff briefed the President's Privacy and Civil Liberties Board on the OIG's review of the FBI's use of national security letters and Section 215 orders for business records.

Legislation and Regulations

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

During this reporting period, the OIG reviewed a variety of legislation, including the *Whistleblower Protection Enhancement Act of 2007*, the *Intelligence Authorization Act for Fiscal Year 2007*, the *Improving America's Security Act*, and the *Freedom of Information Act Amendments of 2007*.

Statistical Information

Audit Statistics

Audit Summary

During this reporting period, the Audit Division issued 106 audit reports containing more than $560 million in questioned costs and more than $170 million in funds to be put to better use and made 420 recommendations for management improvements. Specifically, the Audit Division issued 27 internal reports of Department programs funded at more than $26 billion; 17 external reports of contracts, grants, and other agreements funded at more that $94 million; and 62 *Single Audit Act* audits. In addition, the Audit Division issued seven Notifications of Irregularities and one Management Improvement Memorandum.

Funds Recommended to Be Put to Better Use

Audit Reports	Number of Audit Reports	Funds Recommended to Be Put to Better Use
No management decision made by beginning of period	4	$3,648,849
Issued during period	3	$170,599,707
Needing management decision during period	7	$174,248,556
Management decisions made during period:		
◆ Amounts management agreed to put to better use[1]	2[2]	$109,911,010
◆ Amounts management disagreed to put to better use	0	$0
No management decision at end of period	6	$64,337,546

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

[2] *One audit report was not resolved during this reporting period because management has agreed with some, but not all, of the funds recommended to be put to better use in the audit.*

Audits With Questioned Costs

Audit Reports	Number of Audit Reports	Total Questioned Costs (including unsupported costs)	Unsupported Costs
No management decision made by beginning of period	14	$10,396,267	$3,839,006
Issued during period	28	$560,367,786	$5,076,367
Needing management decision during period	42	$570,764,053	$8,915,373
Management decisions made during period:			
◆ Amount of disallowed costs[1]	23[2]	$269,391,578	$4,191,797
◆ Amount of costs not disallowed	0	$0	$0
No management decision at end of period	20	$301,372,475	$4,723,576

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

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

Audits Involving Recommendations for Management Improvements

Audit Reports	Number of Audit Reports	Total Number of Management Improvements Recommended
No management decision made by beginning of period	25	73
Issued during period	98	420
Needing management decision during period	123	493
Management decisions made during period:		
◆ Number management agreed to implement[1]	89 [2]	346
◆ Number management disagreed with	0	0
No management decision at end of period	40	147

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

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

Audit Follow-Up

OMB Circular A-50

OMB Circular A-50, *Audit Follow-Up*, requires audit reports to be resolved within 6 months of the audit report issuance date. The OIG's Audit Division monitors the status of open audit reports to track the audit resolution and closure process. As of March 31, 2007, the OIG closed 115 audit reports and was monitoring the resolution process of 337 open audit reports.

Unresolved Audits

Audits Over 6 Months Old Without Management Decisions

As of March 31, 2007, the following audits had no management decision or were in disagreement:

- City of Carpentersville, Illinois
- COPS Grant to the City of Dunedin, Florida, Police Department
- COPS Grants to the Picuris Pueblo, New Mexico, Police Department
- COPS Grants to the Navajo Department of Resource Environment, Window Rock, Arizona
- COPS Grants to the Passamaquoddy Tribe and Pleasant Point Reservation Police Department, Perry, Maine
- USMS Intergovernmental Service Agreement for Detention Facilities with the Central Virginia Regional Jail
- USMS Intergovernmental Service Agreement for Detention Facilities with the Blount County, Tennessee, Sheriff's Office
- USMS Intergovernmental Service Agreement for Detention Facilities with the Cumberland County Jail, Portland, Maine
- USMS Intergovernmental Service Agreement for Detention Facilities with the Hamilton County, Tennessee, Silverdale Correctional Facility
- USMS Intergovernmental Service Agreement for Detention Facilities with the Western Tidewater Regional Jail, Suffolk, Virginia
- Use of Equitable Sharing of Assets by the Baltimore County, Maryland, Police Department
- Use of Equitable Sharing of Assets by the Baltimore City, Maryland, Police Department

Quality Control

Every 3 years the OIG's Audit Division is required by the Government Auditing Standards issued by the Comptroller General of the United States to undergo a quality control review by a separate external entity. In February 2007, the Federal Deposit Insurance Corporation (FDIC) OIG completed its external quality control review of the OIG's Audit Division. The FDIC OIG issued an unmodified opinion stating that the system of quality control for the OIG audit function was designed in accordance with the quality standards established by the President's Council on Integrity and Efficiency (PCIE).

In addition, the OIG Audit Division completed an external quality control review of the

Department of Veterans Affairs (VA) OIG Office of Audit. We issued an unmodified opinion stating that the system of quality control for the VA OIG audit function was designed in accordance with the quality standards established by the PCIE.

Evaluation and Inspections Statistics

The chart below summarizes the Evaluation and Inspections Division's (E&I) accomplishments for the 6-month reporting period ending March 31, 2007.

E&I Workload Accomplishments	Number of Reviews
Reviews active at beginning of period	6
Reviews initiated	5
Final reports issued	3
Reviews active at end of reporting period	8

Unresolved Reviews

DOJ Order 2900.10, *Follow-up and Resolution Policy for Inspection Recommendations by the OIG*, requires reports to be resolved within 6 months of the report issuance date. As of March 31, 2007, there were no unresolved recommendations that meet this criterion.

Investigations Statistics

The following chart summarizes the workload and accomplishments of the Investigations Division during the 6-month period ending March 31, 2007.

Source of Allegations	
Hotline (telephone and mail)	777
Other sources	3,752
Total allegations received	4,529
Investigative Caseload	
Investigations opened this period	201
Investigations closed this period	203
Investigations in progress as of 3/31/07	372
Prosecutive Actions	
Criminal indictments/informations	36
Arrests	35
Convictions/Pleas	64
Administrative Actions	
Terminations	9
Resignations	65
Disciplinary action	13
Monetary Results	
Fines/Restitutions/Recoveries	$663,907

Integrity Awareness Briefings

OIG investigators conducted 187 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 8,600 employees.

Appendix 1

Acronyms and Abbreviations

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

ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
BOP	Federal Bureau of Prisons
CODIS	Combined DNA Index System
COPS	Office of Community Oriented Policing Services
DEA	Drug Enforcement Administration
Department	U.S. Department of Justice
DHS	Department of Homeland Security
EOUSA	Executive Office for U.S. Attorneys
FBI	Federal Bureau of Investigation
FISA	*Foreign Intelligence Surveillance Act*
FISMA	*Federal Information Security Management Act*
FY	Fiscal year
ICE	Immigration and Customs Enforcement
IRS	Internal Revenue Service
IT	Information technology
JMD	Justice Management Division
NSL	National Security Letters
OFDT	Office of the Federal Detention Trustee
OIG	Office of the Inspector General
OJP	Office of Justice Programs
OVC	Office for Victims of Crime
OVW	Office on Victims Against Women
OMB	Office of Management and Budget
NIJ	National Institute of Justice
NSA	National Security Agency
Patriot Act	*USA Patriot Act*
Patriot Reauthorization Act	*USA Patriot Improvement and Reauthorization Act of 2005*
USAO	U.S. Attorneys' Offices
USMS	U.S. Marshals Service

Appendix 2

Glossary of Terms

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

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

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

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

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

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

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

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

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

Appendix 3

Evaluation and Inspections Division Reports

October 1, 2006 – March 31, 2007

Follow-up Review of the Critical Incident Response Plans of USAOs

Review of the FBI's Use of National Security Letters (joint effort with Oversight and Review Division)

Review of the FBI's Use of Section 215 Orders for Business Records (joint effort with Oversight and Review Division)

Appendix 4

Audit Division Reports

October 1, 2006 – March 31, 2007

INTERNAL AND EXTERNAL AUDIT REPORTS

Assets Forfeiture Fund and Seized Assets Deposit Fund Annual Financial Statement for FY 2006

BOP Management of the Medical Services Contract with Medical Development International, Butner, North Carolina

ATF's Annual Financial Statement for FY 2006

Compliance with Standards Governing CODIS Activities at the Alabama Department of Forensic Services

Compliance with Standards Governing CODIS Activities at the Wisconsin State Crime Laboratory, Milwaukee, Wisconsin

Cooperation of SCAAP Recipients in the Removal of Criminal Aliens from the United States

COPS Grants Awarded to the Utah Department of Public Safety

Crime Victims Compensation Program Grant to the Oklahoma Crime Victims Compensation Board

The DEA's Annual Financial Statement for FY 2006

Efforts to Prevent, Identify, and Recover Improper and Erroneous Payments by Selected Department Components

The FBI's Annual Financial Statement for FY 2006

The BOP's Annual Financial Statement for FY 2006

Federal Prison Industries, Inc., Annual Financial Statement for FY 2006

Independent Evaluation of the FBI's Intelligence Community Information Security Program and Practices Pursuant to FISMA

OJPs' Annual Financial Statement for FY 2006

OJP National Law Enforcement and Corrections Technology Centers

OVC Identity Theft and Passport Initiative Administered by the Office of the Ohio Attorney General

OVW Grant Awarded to the West Virginia Coalition Against Domestic Violence

Offices, Boards and Divisions Annual Financial Statement for FY 2006

OJP BJA Republican National Convention Grant to the City of New York Police Department

OJP BJA Assistance Residential and Substance Abuse Treatment Formula Grant to the Oklahoma District Attorneys Council

OJP NIJ Solving Cold Cases with DNA Grant Awarded to the City of North Miami, Florida

OJP OJJDP Grants to the State of Oklahoma, Office of Juvenile Affairs

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

Oversight of Intergovernmental Agreements by the USMS and OFDT

Progress Report on Development of the Integrated Wireless Network in the Department

Review of the FBI's Headquarters Information System Controls Environment for FY 2006

Review of the Department's Consolidated Information System General Controls Environment for FY 2006

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

STOP Violence Against Women Formula Grant to the Louisiana Commission on Law Enforcement

STOP Violence Against Women Formula Grant to the Oklahoma District Attorney Council

The Department's Grant Closeout Process

The Department's Internal Controls Over Terrorism Reporting

The DEA's Handling of Cash Seizures

The DEA's International Operations

The FBI's Control Over Weapons and Laptop Computers Follow-up Audit

The National Court-Appointed Special Advocate Program

The USMS's Management of the Justice Prisoner and Alien Transportation System

The Department's Annual Financial Statement for FY 2006

The USMS's Annual Financial Statement for FY 2006

Use of Equitable Sharing Assets by the Norwalk, Connecticut, Police Department

Use of Equitable Sharing Assets by the Philadelphia, Pennsylvania, District Attorney's Office

Use of Equitable Sharing Revenues by the Iowa Department of Public Safety, Des Moines, Iowa

Working Capital Fund Annual Financial Statement for FY 2006

SINGLE AUDIT ACT REPORTS OF DEPARTMENT OF JUSTICE ACTIVITIES

October 1, 2006 – March 31, 2007

13th Judicial District Drug Task Force, Cookeville, Tennessee

Algaaciq Tribal Government, St. Mary's, Alaska

American Bar Association Fund for Justice and Education, Chicago, Illinois

Beyond Missing, Inc., Greenbrae, California

Big Valley Rancheria Band of Pomo Indians, Lakeport, California

Cahto Tribe of Laytonville Rancheria, California

Calhoun County Commission, Anniston, Alabama

Church World Service, Inc., Elkhart, Indiana

City and County of San Francisco, California

City of Chicago, Illinois

City of East St. Louis, Illinois

City of Henderson, Nevada

City of Hillsboro, Oregon

City of Huntington Park, California

City of Knoxville, Tennessee

City of Mason City, Iowa

City of Miami Springs, Florida

City of North Las Vegas, Nevada

City of Selma, Alabama

City of Tampa, Florida

City of Terre Haute, Indiana

Commonwealth of the Northern Mariana Islands

Elko Band Council, Elko, Nevada

Etowah County Commission, Gadsden, Alabama

Fallon Paiute-Shoshone Tribe, Fallon, Nevada

Georgia State University Research Foundation, Inc., Atlanta, Georgia

Government of Guam, Hagatna, Guam, FY 2003

Government of Guam, Hagatna, Guam, FYs 2004 and 2005

Hawaii Community Foundation, Honolulu, Hawaii

Henry County Board of Commissioners, McDonough, Georgia

Hoonah Indian Association, Hoonah, Alaska

Indian Township Tribal Government, Princeton, Maine

Las Vegas Paiute Tribe, Las Vegas, Nevada

Laurens County, Dublin, Georgia

Lower Elwha Klallam Tribe, Port Angeles, Washington

National Association of Police and Athletic Activities Leagues, Inc., Jupiter, Florida

National Council of Juvenile and Family Court Judges, Inc., Reno, Nevada

Native Village of Barrow, Alaska

Native Village of St. Michael, Alaska

Nevada Urban Indians, Inc., Reno, Nevada

Newtok Traditional Council, Newtok, Alaska

Pleasant Point Passamaquoddy Tribal Council, Perry, Maine

Porter County, Valparaiso, Indiana

Safe & Sound, Inc., Milwaukee, Wisconsin

Sangamon County, Springfield, Illinois

Shoshone-Paiute Tribes of Duck Valley Reservation, Owyhee, Nevada

Sioux County, Orange City, Iowa

State of Alabama, Montgomery, Alabama, FY 2004

State of Alabama, Montgomery, Alabama, FY 2005

State of Alaska, Juneau, Alaska

State of Florida, Tallahassee, Florida

State of Georgia, Atlanta, Georgia

State of Iowa, Des Moines, Iowa

State of Nevada

Tanana Chiefs Conference, Fairbanks, Alaska

The Paul & Lisa Program, Inc., Essex, Connecticut

University of Delaware, Newark, Delaware

University of Hawaii, Honolulu, Hawaii

University of Maine System, Bangor, Maine

University of New Haven, West Haven, Connecticut

Village of Forest Park, Illinois

Yomba Shoshone Tribe, Austin, Nevada

Audit Division Reports

October 1, 2006 – March 31, 2007

Quantifiable Potential Monetary Benefits

Audit Report	Questioned Costs	Unsupported Costs	Funds Put to Better Use
13th Judicial District Drug Task Force, Cookeville, Tennessee	$27,320	$27,320	
Algaaciq Tribal Government, St. Mary's, Alaska	$34,419	$34,419	
American Bar Association Fund for Justice and Education, Chicago, Illinois	$93,180	$93,180	
BOP Management of the Medical Services Contract with Medical Development International, Butner, North Carolina	$2,428,345	$2,428,345	
Church World Service, Inc., Elkhart, Indiana	$73,036	$73,036	
City and County of San Francisco, California	$253,500	$253,500	
City of Knoxville, Tennessee	$19,873	$19,873	
City of Mason City, Iowa	$74,656	$74,656	
City of North Las Vegas, Nevada	$84,255	$84,255	
City of Selma, Alabama	$5,100	$5,100	
COPS Grants Awarded to the Utah Department of Public Safety	$59,919	$11,160	
Elko Band Council, Elko, Nevada	$7,830	$7,830	
Fallon Paiute-Shoshone Tribe, Fallon, Nevada	$38,351	$38,351	
Government of Guam, Hagatna, Guam, FY 2003	$277,427	$277,427	
Hawaii Community Foundation, Honolulu, Hawaii	$1,096	$757	
National Association of Police and Athletic Activities Leagues, Inc., Jupiter, Florida	$2,770	$2,770	
OVC Identity Theft and Passport Initiative Administered by the Office of the Ohio Attorney General	$154,657	$146,320	
OJP BJA Republican National Convention Grant to the City of New York Police Department	$49,699	$47,307	
OJP National Law Enforcement and Corrections Technology Centers	$697,005	$472,069	

Audit Report	Questioned Costs	Unsupported Costs	Funds Put to Better Use
OJP Southwest Border Prosecution Initiative Funding Received by the Yuma County Attorney's Office, Yuma, Arizona	$284,338	$200,147	$17,500
State of Alabama, Montgomery, Alabama, FY 2004	$28,333	$28,333	
STOP Violence Against Women Formula Grant to the Louisiana Commission on Law Enforcement	$51,972	$51,972	
The Department's Grant Closeout Process	$554,869,315		$170,395,988
The Paul & Lisa Program, Inc., Essex, Connecticut	$5,010	$5,010	
University of Maine System, Bangor, Maine	$21,535	$21,535	
University of New Haven, West Haven, Connecticut	$133,284	$133,284	
Use of Equitable Sharing Assets by the Philadelphia, Pennsylvania District Attorney's Office	$1,591	$1,591	$186,219
Use of Equitable Sharing Revenues by the Iowa Department of Public Safety, Des Moines, Iowa	$589,970	$536,820	
Total	***$560,367,786***	***$5,076,367***	***$170,599,707***

Appendix 5

Reporting Requirements Index

The IG Act specifies reporting requirements for semiannual reports. The requirements are listed below and indexed to the applicable pages.		
IG Act References	**Reporting Requirements**	**Page**
Section 4(a)(2)	Review of Legislation and Regulations	45
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	7-44
Section 5(a)(2)	Significant Recommendations for Corrective Actions	7-43
Section 5(a)(3)	Prior Significant Recommendations Unimplemented	48-49
Section 5(a)(4)	Matters Referred to Prosecutive Authorities	22-23, 27-28, 32-33, 35-37, 40, 42
Section 5(a)(5)	Refusal to Provide Information	None
Section 5(a)(6)	Listing of Audit Reports	53-58
Section 5(a)(7)	Summary of Significant Reports	7-43
Section 5(a)(8)	Audit Reports — Questioned Costs	47
Section 5(a)(9)	Audit Reports — Funds to Be Put to Better Use	46
Section 5(a)(10)	Prior Audit Reports Unresolved	48
Section 5(a)(11)	Significant Revised Management Decisions	None
Section 5(a)(12)	Significant Management Decisions with which the OIG Disagreed	None

Report Waste, Fraud, Abuse, or Misconduct

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

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

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

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

Report Violations of Civil Rights and Civil Liberties

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

Civil Rights and Civil Liberties Complaints
Office of the Inspector General

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

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

On-Line Report Availability

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

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

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

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

Or call: (202) 616-4550

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

Established April 14, 1989