

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

Office of the Inspector General Semiannual Report to Congress



October 1, 2005–March 31, 2006

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

Message From the Inspector General

This semiannual report summarizes the work of the Office of the Inspector General (OIG) from October 1, 2005, through March 31, 2006. The audits, inspections, investigations, special reviews, and other activities highlighted in this report illustrate our ongoing commitment to promote accountability, efficiency, and effectiveness in the programs and operations of the Department of Justice (Department).

Over the past 6 months, we continued to concentrate much of our efforts on the Department's top management and performance challenges, including counterterrorism, the sharing of intelligence and law enforcement information, and attempts to upgrade information technology (IT) systems. For example, during this reporting period we examined the Federal Bureau of Investigation's (FBI) development of its Sentinel electronic case management system and the FBI's efforts to protect the nation's seaports. We also assessed the FBI's handling of a matter that involved a Portland, Oregon, lawyer whose fingerprints were misidentified by the FBI as matching a fingerprint found on a bag of detonators connected with the March 2004 Madrid train bombing. In addition, as part of our semiannual report to Congress pursuant to Section 1001 of the *USA PATRIOT Act* (Patriot Act), we examined the FBI's process for reporting possible violations involving its intelligence activities to the Intelligence Oversight Board.

We completed significant reviews of other Department components as well, including an examination of the U.S. Attorneys' Offices' (USAO) use of intelligence research specialists to analyze and share terrorism-related information and an audit of the Office of Community Oriented Policing Services' (COPS) management of a methamphetamine grant program. We also continued to investigate various allegations of criminal and administrative misconduct by Department employees and contractors.

During this reporting period, the OIG began a review required by Congress in the *USA Patriot Improvement and Reauthorization Act of 2005*. That legislation directs the OIG to review the FBI's use of its authorities to issue National Security Letters and obtain orders under the *Foreign Intelligence Surveillance Act* (FISA) for business records.

In addition, in January 2006 legislation was enacted that increases the statutory penalty for sexual abuse of federal inmates by correctional staff and expands federal jurisdiction to sex abuse and contraband cases involving federal inmates housed in non-federal correctional facilities. The OIG has investigated many allegations of sexual abuse of federal inmates and introduction of contraband into contract facilities, and we believe the increased penalties can help deter this criminal conduct.

We appreciate the positive response we receive regarding our work from the Department and Congress. We also appreciate their continued support as we strive to assist the Department in increasing the efficiency and effectiveness of its operations.

Finally, I want to express my gratitude to the OIG staff who work diligently to fulfill the OIG's critical mission. They are dedicated public servants who deserve great credit for helping improve the work of the Department and the federal government.

A handwritten signature in dark ink, reading "Glenn A. Fine".

Glenn A. Fine
Inspector General
April 28, 2006

Table of Contents

Highlights of OIG Activities	1
OIG Profile	4
Multicomponent Audits, Reviews, and Investigations	6
Federal Bureau of Investigation	12
Office of Justice Programs	19
Bureau of Alcohol, Tobacco, Firearms and Explosives	23
Federal Bureau of Prisons	26
U.S. Marshals Service	29
Drug Enforcement Administration	31
Other Department Components	33
Office of Community Oriented Policing Services	33
U.S. Attorneys' Offices	35
Top Management Challenges	37
Congressional Testimony	38
Legislation and Regulations	38
Statistical Information	39
<i>Audit Statistics</i>	39
Funds Recommended for Better Use	39
Questioned Costs	40
Management Improvements	40
Audit Follow-Up	41
Unresolved Audits	41
<i>Evaluation and Inspections Statistics</i>	41
<i>Investigations Statistics</i>	42
Appendices	
Acronyms and Abbreviations	43
Glossary of Terms	44
Evaluation and Inspections Division Reports	46
Audit Division Reports	47
Reporting Requirements Index	52

Highlights of OIG Activities

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

Statistical Highlights

October 1, 2005 - March 31, 2006

Allegations Received by the Investigations Division	4,088
Investigations Opened	185
Investigations Closed	211
Arrests	48
Indictments/Informations	52
Convictions/Pleas	47
Administrative Actions	80
Fines/Restitutions/Recoveries	\$1.8 million
Audit Reports Issued	89
Questioned Costs	\$31 million
Funds Put to Better Use	\$50 million
Recommendations for Management Improvements	351

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

- ◆ The FBI's Sentinel Case Management System. The OIG issued an audit of the FBI's plans to develop the Sentinel case management system to replace the failed Virtual Case

File effort. Sentinel is intended to enable the FBI to move from a paper-based reporting system to an electronic records system and maximize the FBI's ability to use and share information. Our audit found that the FBI has developed IT planning procedures that, if implemented as designed, can help the FBI successfully complete Sentinel. However, we also identified several project concerns that require action and continued monitoring, including incomplete staffing of the Program Management Office, the FBI's ability to reprogram funds to complete the second phase of the project without jeopardizing its mission-critical operations, Sentinel's capability to share information with external intelligence and law enforcement agencies, and how the FBI tracks and controls Sentinel's costs. The OIG provided seven recommendations regarding these concerns.

- ◆ The FBI's Handling of the Brandon Mayfield Matter. The OIG reviewed the FBI's conduct in connection with the identification of a fingerprint found on evidence from the March 2004 terrorism attack on commuter trains in Madrid, Spain. FBI fingerprint examiners erroneously concluded that the fingerprint belonged to Brandon Mayfield, an attorney in Portland, Oregon. Mayfield was arrested as a material witness but released 2 weeks later when the Spanish National Police identified an Algerian national as the source of the fingerprint. We found several factors that caused the FBI's fingerprint misidentification, including the unusual similarity between Mayfield's fingerprint and the fingerprint found on the evidence, errors committed by FBI examiners that could have been prevented through a more rigorous

application of latent fingerprint identification, and the FBI's decision to disregard information from the Spanish National Police that Mayfield's fingerprints reached a "negative" matching conclusion. We made a series of recommendations to help the FBI address the laboratory issues raised by the Mayfield case.

- ◆ The FBI's Efforts to Protect the Nation's Seaports. The OIG audited the FBI's efforts to help secure the nation's seaports. We found that during the past 3 years the FBI has taken steps to enhance its capability to identify, prevent, and respond to terrorism attacks in the maritime domain. However, the OIG also identified several actions the FBI should take to enhance seaport security, including increasing coordination with other agencies who share responsibility for maritime security, assessing the threat and risk of maritime terrorism compared to other terrorism threats, and improving the database that the FBI uses to collect and manage data concerning the number of suspicious incidents or terrorism threats involving seaports. We provided 18 recommendations to enhance the FBI's efforts to secure U.S. seaports.
- ◆ COPS' Methamphetamine Initiative. The OIG examined COPS' administration of the Department's grant program to stem the production, distribution, and use of methamphetamine. Over the past 8 years, Congress has appropriated more than \$200 million for grants to state and local law enforcement agencies to combat methamphetamine. The OIG review found significant deficiencies in COPS' administration of the methamphetamine grant program, in its monitoring of grantee activities, and in the way individual grantees administered their grants.
- ◆ The U.S. Attorneys' Offices' Intelligence Research Specialists. The OIG evaluated the role and functions of USAO intelligence research specialists and found that individually the specialists made valuable contributions to the USAOs' antiterrorism efforts. However, their overall effectiveness could be increased through improved coordination and guidance at the regional and Departmental levels. We made eight recommendations to the Executive Office for U.S. Attorneys (EOUSA) to improve the USAOs' use of intelligence research specialists.
- ◆ The Bureau of Prisons' Pharmacy Services. The OIG evaluated the Bureau of Prisons' (BOP) attempts to reduce increasing costs of prescription medications and assessed whether the BOP ensures adequate controls and safeguards over prescription medications. We concluded that the BOP could reduce prescription medication costs associated with waste from unused prescriptions, which totaled an estimated \$2.81 million in fiscal year (FY) 2004. Our report contained 13 recommendations for the BOP to improve the administration of its Pharmacy Services, including fully implementing several cost-savings initiatives.
- ◆ Civil Rights and Civil Liberties Reviews. As directed by Section 1001 of the Patriot Act, the OIG receives and reviews complaints alleging civil rights and civil liberties abuses by Department employees. During this reporting period, the OIG issued its eighth report summarizing its duties under Section 1001. Included in the report was our review of the FBI's reporting on possible violations to the President's Intelligence Oversight Board (IOB). We determined that in FYs 2004 and 2005 the FBI reported to the IOB possible intelligence violations in 108 matters. These possible violations fell into one of the following three categories: 1) improper utilization of authorities under FISA, 2) failure to adhere to Attorney General Guidelines, or 3) improper utilization of authorities involving National Security Letters.

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 report include:

- ◆ An OIG investigation led to the indictment of a Drug Enforcement Administration (DEA) special agent for allegedly stealing more than \$200,000 from money seized from drug organization couriers.
- ◆ Several individuals were indicted on charges of conspiracy, mail fraud, wire fraud, theft of government property, false statements, and obstruction of justice after OIG investigators found that they spent more than \$330,000 of a Bureau of Justice Assistance (BJA) grant – awarded for the creation of a prison re-entry program – for personal use, then created false documents to cover up their activities.
- ◆ A BOP senior correctional officer pled guilty to charges of bribery after an OIG investigation determined that the officer procured cell phones, drugs, and other contraband for prisoners in exchange for bribe payments in excess of \$12,000.
- ◆ An OIG investigation led to the guilty plea to wire fraud by a civilian assigned to a Xerox contract with the Los Angeles USAO. The individual ordered excess toner and other printing supplies under the guise of the Department's fixed price contract, then stole over \$700,000 in those supplies and sold the merchandise for his own profit.
- ◆ A DEA contractor and contractor employee were convicted of bid rigging after an OIG investigation revealed that they submitted

three bids – all at different amounts – to perform electrical work for the DEA. The contractor and employee were debarred from all government contracts.

Ongoing Work

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

- ◆ Coordination of the Department's Crime Task Force Investigations
- ◆ Review of the Department's IT Initiatives
- ◆ Progress Toward Biometric Fingerprint Interoperability
- ◆ The Department's Internal Controls Over Terrorism Reporting
- ◆ Review of the Ojeda Rios Shooting in Puerto Rico
- ◆ FBI Reports of Alleged Abuse of Military Detainees
- ◆ The FBI's Handling of Chinese Intelligence Asset Katrina Leung
- ◆ Follow-up Review of the FBI's Control Over Weapons and Laptop Computers
- ◆ Review of the FBI's Response to Recommendations to Improve its Internal Security in Light of the Robert Hanssen Case
- ◆ Bureau of Alcohol, Tobacco, Firearms and Explosives' (ATF) Violent Crime Impact Teams
- ◆ BOP Controls Over Inmate Mail
- ◆ The U.S. Marshals Service's (USMS) Justice Prisoner and Alien Transportation System
- ◆ The DEA's Drug Diversion Control Program
- ◆ DEA Controls Over Cash Seizures

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, 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 FY 2006, the OIG's direct appropriation is

\$67.9 million, and the OIG expects to earn an additional \$3.3 million in reimbursements.

As required by Section 5 of the *Inspector General Act of 1978* (IG Act), as amended, this *Semiannual Report to Congress* reviewing the accomplishments of the OIG for the 6-month period of October 1, 2005, through March 31, 2006, is to be submitted no later than April 30, 2006, to the Attorney General for his review. The Attorney General is required to forward the report to Congress no later than May 31, 2006, 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 audits, reviews, and investigations involve more than one Department component.

Reports Issued

Civil Rights and Civil Liberties Reviews

Section 1001 of the 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 2006, the OIG issued its eighth report summarizing its Section 1001 activities.

The report, covering the period from July 1, 2005, to December 31, 2005, described complaints we received under this section, cases opened for investigation, the status of these cases, and reviews we completed relating to our Section 1001 responsibilities.

The report provided an update on the discipline imposed by the BOP on corrections staff who worked at a federal prison in Brooklyn, New York, where we found abuse of detainees arrested in connection with the government's investigation into the September 11 terrorism attacks. According to the BOP, discipline was imposed on 13 staff members: 2 were terminated from the

BOP, 8 were suspended for periods ranging from 2 to 30 days, and 3 were demoted.

In addition, the report presented the results of an OIG review of the FBI's reporting on possible violations to the President's Intelligence Oversight Board (IOB). Under the process, FBI employees self-report potential violations to its Office of the General Counsel, which reviews the possible violations to determine whether reporting to the IOB is required. For FYs 2004 and 2005, the FBI reported to the IOB potential intelligence violations in 108 matters.

Examples of the 108 possible violations that the FBI reported to the IOB in FYs 2004 and 2005 include FBI agents intercepting communications outside the scope of the order from the Foreign Intelligence Surveillance Court, a special court created by FISA; FBI agents continuing investigative activities after the authority for the specific activity expired; and the FBI receiving information that was not requested by a National Security Letter. Not all possible violations were attributable solely to FBI conduct. According to the data we reviewed, third parties such as telephone companies were involved in or responsible for possible violations in at least one-quarter of the cases in both years we examined.

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 financial statement audit reports based on the work performed by independent public accountants.

The Department received an unqualified opinion on its FYs 2005 and 2004 financial statements. The Department had previously received a disclaimer on its FY 2004 financial statements due to a disclaimer on the FY 2004 financial statements of Office of Justice Programs (OJP). However, due to restatements and re-audits of its FYs 2004 and 2003 financial statements, OJP obtained unqualified opinions on those two financial statements, as well as on its FY 2005 financial statements. Another component, ATF, had previously received a qualified opinion on its FY 2004 financial statements. ATF provided sufficient supporting documentation for its FY 2004 accounts payable accrual during FY 2005 to support unqualified opinions on its FYs 2005 and 2004 financial statements. The other eight Department components received unqualified opinions on both their FY 2005 and 2004 financial statements.

At the consolidated level, we reported two material weaknesses, compared to two material weaknesses and one reportable condition in FY 2004. Both material weaknesses in FY 2005 are repeat issues from the previous year, although the elements of the two findings varied from last year. The first material weakness involved serious issues at the component level, including the USMS's internal control framework and management and recording of real property; OJP's grant advance and payable estimation processes and financial reporting, monitoring, analysis, and documentation; ATF's controls

over its accounts payable accrual; and the FBI's financial reporting and property control.

The second consolidated material weakness, which relates to information systems, was elevated from a reportable condition last year. We found new and continued deficiencies in 8 of the 10 components, as well as weaknesses in the Department's consolidated information system general controls environment. We determined that general controls in place for the consolidated information system general controls environment were adequate to safeguard the programs and data files from unauthorized access and modification, except as noted in the overall reportable condition. Therefore, a moderate level of reliance can be placed upon the general controls associated with the consolidated information system general controls environment to promote financial statement integrity and reliability. However, the reportable condition summarized 13 issues categorized in the areas of security program, access controls, and system software. We provided 14 recommendations for improving the consolidated information system general controls environment, including monitoring background investigations and reinvestigations for contractors and employees, reviewing the Justice Secure Remote Access system audit logs at a minimum of once per week, implementing the Department's Information Technology Security Standard 3.1, and implementing the required vendor security patches on all hosts.

At the component level, the total number of material weaknesses was unchanged from 10 in FY 2004. However, the number of reportable conditions decreased significantly from 13 in FY 2004 to 8 this year. Two components, the DEA and the Federal Prison Industries, Inc., had no material weaknesses, reportable conditions, or compliance issues.

We reported that the Department still lacks sufficient automated systems to readily support ongoing accounting operations and financial

statement preparation. In addition, a shortage exists of trained financial management personnel available to perform certain internal control functions related to the financial reporting process. This shortage inhibits the ability of both Department and component management to assess financial reporting risk; design, communicate, and implement appropriate control activities; and monitor the financial reporting process. Many tasks still must be performed manually at interim periods and at year's end, requiring extensive efforts on the part of financial and audit personnel. These significant, costly, and time-intensive manual efforts will continue

to be necessary for the Department and its components to produce financial statements until automated, integrated processes and systems are implemented that readily produce the necessary information throughout the year. We agree with the Department's efforts to obtain funding to implement a unified financial management system, supported by consistent, standardized business practices across the Department.

The table below compares FYs 2005 and 2004 audit results for the Department's consolidated audit as well as for the 10 individual component audits.

Comparison of FY 2005 and FY 2004 Audit Results						
Reporting Entity	Auditors' Opinion on Financial Statements		Number of Material Weaknesses		Number of Reportable Conditions	
	2005	2004	2005	2004	2005	2004
Consolidated Department of Justice	Unqualified	Unqualified ¹	2	2	0	1
Offices, Boards and Divisions	Unqualified	Unqualified	0	0	1	2
Assets Forfeiture Fund and Seized Asset Deposit Fund	Unqualified	Unqualified	0	0	1	1
Federal Bureau of Investigation	Unqualified	Unqualified	2	2	1	1
Drug Enforcement Administration	Unqualified	Unqualified	0	0	0	1
Office of Justice Programs	Unqualified	Unqualified ¹	3	5	1	1
U.S. Marshals Service	Unqualified	Unqualified	3	2	1	2
Federal Bureau of Prisons	Unqualified	Unqualified	0	0	1	1
Federal Prison Industries, Inc.	Unqualified	Unqualified	0	0	0	1
Working Capital Fund	Unqualified	Unqualified	0	0	2	2
Bureau of Alcohol, Tobacco, Firearms and Explosives	Unqualified	Unqualified ²	2	1	0	1
Component Totals			10	10	8	13
¹ Originally issued as a disclaimer of opinion, the opinion was reissued in FY 2005 to an unqualified opinion after re-audits were performed on OJP's FY 2004 and FY 2003 financial statements.						
² Originally issued as a qualified opinion, the opinion was reissued in FY 2005 to an unqualified opinion after additional test work was performed on ATF's accounts payable accrual.						

The Department's Management of Information Technology

The Department's IT budget for FY 2005 is \$2.2 billion for 320 systems, including 22 major systems that cover more than one Department component. To more effectively manage its IT investments in compliance with legislation and regulations, the Department is in the early stages of developing Enterprise Architecture and Information Technology Investment Management (ITIM) processes.

The OIG's Audit Division performed an audit to determine if the Department is effectively managing its Enterprise Architecture and ITIM efforts. The OIG has identified IT systems planning and utilization as one of the Department's Top 10 Management Challenges, and the Department has faced significant obstacles in meeting this challenge.

Our audit found that the Department is in the process of developing both Enterprise Architecture and ITIM processes based on Department-developed frameworks, and the Department has begun to improve its oversight and guidance of the components' Enterprise Architectures and ITIM processes. However, additional oversight is needed to ensure the success of the Capability Delivery Model and the IT Strategic Management (ITSM) framework.

We made seven recommendations for improving the Department's IT management, including completing the Department-wide Enterprise Architecture, providing guidance to components for the development and maintenance of Enterprise Architectures, tracking and reviewing the development of component-level Enterprise Architectures, implementing the phases outlined by the ITSM framework, ensuring that components requiring ITIM processes develop them, assisting components in developing and implementing ITIM processes,

and establishing a clear schedule for completing the ITSM framework and a mature ITIM process. The Department concurred with all of our recommendations.

The Department's Information Security Program Pursuant to FISMA

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

For FY 2005, we reviewed the security programs of four major components within the Department: the FBI, BOP, DEA, and Justice Management Division. We also reviewed four component mission-critical systems: the FBI's Automated Case Support (classified system), the DEA's El Paso Intelligence Center Information (classified system), the BOP's Inmate Telephone System II (sensitive but unclassified system), and the DEA's El Paso Intelligence Center Seizure (sensitive but unclassified system). We submitted a response to the OMB questionnaire on October 7, 2005, which provided updated information about the overall effectiveness of the Department's IT security program. Separate reports will be issued in FY 2006 for each component and system evaluated.

Investigations

The following are examples of cases involving more than one component that the OIG's

Investigations Division investigated during this reporting period:

- ◆ The OIG's Washington Field Office examined the premature disclosure of a draft press release prepared by the Criminal Division's Child Exploitation and Obscenities Section. The draft release reported on the indictment of four named individuals for transmitting pornographic SPAM through a computer network. The draft release contained the caption, "For Immediate Release, Wednesday, August 24, 2005," and was placed on a national newspaper's blog website on August 24. However, the indictment was not returned until the next day and did not include a fourth individual. The OIG investigation determined that the draft press release was released by the FBI to private entities, and ultimately to the newspaper, because of the lack of proper labeling of the press release as a "draft" during its circulation.
- ◆ The OIG previously investigated a case in which a truck driver in New Jersey filed a claim against the September 11 Victim Compensation Fund for \$1.9 million. The truck driver stated that he suffered personal injuries while making deliveries at the World Trade Center on September 11, 2001. An investigation by the OIG's Fraud Detection Office revealed that he falsified company and medical records, and was not working near the World Trade Center on that day. During this reporting period, the truck driver was sentenced to 30 months' incarceration and 2 years' supervised release following his guilty plea for filing a false claim. The truck driver also settled a civil case against him by agreeing to pay a penalty of \$10,000.

Ongoing Work

Coordination of the Department's Crime Task Force Investigations

As directed by Congress, the OIG is evaluating whether investigations conducted by the Department's crime task forces are well coordinated to ensure officer safety; avoid duplication of effort; and assist state, local, and tribal efforts to reduce violent crime. The review will focus on the FBI's Safe Streets Task Forces, ATF's Violent Crime Impact Teams, DEA's Mobile Enforcement Teams, and USMS's Regional Fugitive Task Forces during FYs 2003, 2004, and 2005.

Reviews of the Department's IT Initiatives

In accordance with the requirements of the Department's FY 2006 Appropriations Conference Report, the OIG was directed to compile and present to the House and Senate Appropriations Committees an inventory of major Department IT systems and report on research, plans, studies, and evaluations that the Department has produced, or is in the process of producing, concerning its information systems. In response the OIG is conducting: 1) an unaudited report of the Department's major IT system investments by investment title/component, investment description, implementation status, and FYs 2005 through 2007 actual and projected costs; 2) an audited verification of the information detailed in the unaudited report; and 3) a report providing details on the Department's research,

plans, studies, and evaluations along with an analysis identifying the depth and scope of the problems the Department has experienced in the formulation of its IT plans.

Progress Toward Biometric Fingerprint Interoperability

The OIG is reviewing the FBI's progress toward achieving interoperability between its Integrated Automated Fingerprint Identification System (IAFIS) and two automated fingerprint systems of the Department of Homeland Security (DHS), the Automated Biometric Identification System (IDENT) and the U.S. Visitor and Immigrant Status Indicator Technology. The review will assess actions the FBI and the Department have taken since the OIG's December 2004 report on the status of IDENT/IAFIS integration.

The Department's Integrated Wireless Network

The Integrated Wireless Network (IWN) is intended to link approximately 80,000 federal, state, and local law enforcement officers and public safety agencies in a secure interoperable wireless service that provides consolidated nationwide integrated communications in support of law enforcement, first responder, and homeland security requirements. The OIG is evaluating the Department's planning and contracting for the IWN by determining whether: 1) the

Department has the structure and process in place to manage and control costs and schedules, 2) the Department's assessment of the vendors' technical and management capabilities ensure that the vendors are able to carry out the project successfully, and 3) legacy communication systems comply with the National Telecommunications and Information Administration's requirements.

The Department's Internal Controls Over Terrorism Reporting

The Department measures its counterterrorism efforts in part by reporting terrorism-related statistics in its performance plans and statistical reports. The OIG initiated an audit to determine if Department components and the Department as a whole accurately report terrorism-related statistics.

Grant Closeout Process Utilized Within the Department

The OIG is reviewing the grant closeout processes used by COPS, OJP, and Office on Violence Against Women. In conducting the audit, the OIG will determine whether the grant closeout processes are adequate to ensure that expired grants are closed in a timely manner; grant funds are drawn down in accordance with federal regulations, Department policy, and the terms and conditions of the grant; and remaining grant funds are deobligated prior to closeout.

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 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 Sentinel Case Management System

In March 2005, the FBI announced plans to develop the Sentinel case management system to replace the failed Virtual Case File effort. The main goal of Sentinel is to enable the FBI to move from a paper-based reporting system to an electronic records system and maximize the FBI's ability to use and share the information in its possession. During this reporting period, the OIG's Audit Division completed an initial audit of the Sentinel project. This audit, the first in a series for the multi-phase project, focused on the FBI's pre-acquisition planning, including its approach to developing the system, management controls over the project, IT management processes, contracting processes, and funding sources.

The OIG found that the FBI has taken important steps to prevent the types of problems encountered in the Virtual Case File project. In reviewing the management processes and

controls the FBI has applied to the pre-acquisition phase of Sentinel, the OIG found that the FBI has developed IT planning processes that, if implemented as designed, can help the FBI successfully complete Sentinel.

The FBI also has made significant improvements in its ability to plan and manage a major IT project. For example, the FBI established sound ITIM processes, developed a more mature Enterprise Architecture, and established a Program Management Office (PMO) specifically for the Sentinel project.

However, we identified several concerns about the project that require action and continued monitoring: 1) the incomplete staffing of the PMO, 2) the FBI's ability to reprogram funds to complete the second phase of the project without jeopardizing its mission-critical operations, 3) Sentinel's ability to share information with external intelligence and law enforcement agencies and provide a common framework for other agencies' case management systems, 4) the

lack of an established Earned Value Management process, 5) the FBI's ability to track and control Sentinel's costs, and 6) the lack of complete documentation required by ITIM.

The OIG made seven recommendations regarding these concerns. The FBI concurred with all of the recommendations.

The FBI's Handling of the Brandon Mayfield Matter

The OIG issued a report on the FBI's conduct in connection with the identification of a fingerprint found on evidence from the March 2004 terrorism attack on commuter trains in Madrid, Spain, that killed almost 200 people and injured more than 1,400. FBI fingerprint examiners erroneously concluded that the fingerprint found on a bag of detonators belonged to Brandon Mayfield, an attorney in Portland, Oregon. As a result of the misidentification, the FBI initiated an investigation of Mayfield that resulted in his arrest as a material witness. Mayfield was released 2 weeks later when the Spanish National Police identified an Algerian national as the source of the fingerprint on the bag. The FBI Laboratory subsequently withdrew its fingerprint identification of Mayfield.

During its review, the OIG's Oversight and Review Division found several factors that caused the FBI's fingerprint misidentification. The unusual similarity between Mayfield's fingerprint and the fingerprint found on the bag (referred to as LFP 17) confused three experienced FBI examiners and a court-appointed expert. However, we also found that FBI examiners committed errors in the examination procedure, and the misidentification could have been prevented through a more rigorous application of several principles of latent fingerprint identification.

For example, the examiners placed excessive reliance on extremely tiny details in the latent fingerprint under circumstances that should have indicated that these features were not a reliable support for the identification. The examiners also overlooked or rationalized several important differences in appearance between the latent print and Mayfield's known fingerprint that should have precluded them from declaring an identification. In addition, we determined that the FBI missed an opportunity to catch its error when the Spanish National Police informed the FBI on April 13, 2004, that it had reached a "negative" conclusion with respect to matching LFP 17 to Mayfield's fingerprints.

Although the OIG determined that religion played no role in the FBI examiners' initial conclusions, we found that by the time the Spanish National Police issued its "negative" conclusion, Laboratory examiners had become aware of information about Mayfield obtained in the course of the Portland Division's investigation, including the fact that he had acted as an attorney for a convicted terrorist, had contacts with suspected terrorists, and was Muslim. We believe that these factors likely contributed to the examiners' failure to sufficiently reconsider the identification after the Spanish National Police raised legitimate questions about it.

We also found that certain facts in affidavits the FBI submitted to the U.S. District Court for the District of Oregon to obtain a material witness warrant and search warrants were misleading. The affidavits contained several inaccuracies and provided an ambiguous description of a meeting between the FBI and the Spanish National Police that led the Court to incorrectly believe that the Spanish National Police agreed with the FBI's identification of Mayfield.

The OIG did not find evidence that the FBI misused any of the provisions of the Patriot Act in conducting its investigation of Mayfield.

However, the increased information sharing permitted by the Patriot Act amplified the consequences of the FBI's fingerprint misidentification.

We made a series of recommendations to help the FBI address the Laboratory issues raised by the Mayfield case. The FBI Laboratory is planning to adopt new procedures that are consistent with a majority of our recommendations.

The FBI's Efforts to Protect the Nation's Seaports

The protection of our nation's seaports and related maritime activities is a shared responsibility among the U.S. Coast Guard, U.S. Customs and Border Protection, and FBI. The FBI, as the lead federal agency for preventing and investigating terrorism, has an overarching role in helping secure the nation's seaports. The FBI's responsibilities are part intelligence and part law enforcement, including assessing the threat of maritime-based terrorism; gathering, analyzing, and sharing information on maritime threats; and maintaining well-prepared tactical capabilities to prevent or respond to maritime-based terrorism.

During their review of the FBI's efforts to prevent and respond to maritime terrorism, the OIG's Audit Division found that since the September 11, 2001, terrorism attacks the FBI has taken steps to enhance its capability to identify, prevent, and respond to terrorism attack at seaports. For example, the FBI has created a centralized maritime security program at FBI Headquarters and, in addition to its counterterrorism tactical teams, has placed enhanced maritime SWAT teams in FBI field offices. In addition, most of the FBI's 56 field offices have Maritime Liaison Agents responsible

for coordinating with other federal agencies on maritime security. However, we found that the FBI does not always assign these agents according to the threat and risk of a terrorism attack on a given seaport. For example, an FBI field office with six significant seaports in its territory has only one maritime liaison agent, while another FBI field office with no strategic ports in its area has five maritime liaison agents.

The OIG also identified several actions the FBI should take to enhance seaport security, including increasing coordination with other agencies who share responsibility for maritime security, assessing the threat and risk of maritime terrorism compared to other terrorism threats, and improving the database that the FBI uses to collect and manage data concerning the number of suspicious incidents or terrorism threats involving seaports.

The OIG review found that the FBI and the Coast Guard have not yet resolved issues regarding their overlapping responsibilities, jurisdictions, and capabilities to handle a maritime terrorism incident. Because the FBI and the Coast Guard share the responsibility for ensuring the safety of U.S. seaports, the FBI needs to come to an agreement with the Coast Guard on each agency's respective roles and authorities.

We also found that the FBI has failed to conduct a threat assessment that indicates where seaports rank among the likely targets of terrorism. This lack of assessment has hampered the FBI's ability to compare the likelihood of various threats and make informed decisions about resource allocation. In addition, we found that the FBI database used to collect information on terrorism threats and suspicious incidents at seaports cannot be easily searched to identify trends in maritime-related suspicious activities or threats. Moreover, the FBI has not ensured that FBI offices enter all required information into this database.

Our report provided 18 recommendations to enhance the FBI's efforts to secure U.S. seaports, including: resolve potential role and incident command conflicts in the event of a maritime terrorism incident through joint exercises and, if necessary, a revised and broadened memorandum of understanding with the Coast Guard; assign Maritime Liaison Agents to critical seaports based on an assessment of the threat and risk of a terrorism attack; assess the threat and risk of maritime terrorism compared to other terrorism threats; and focus intelligence reporting to more comprehensively address potential maritime-related terrorism targets and methods. The FBI agreed with the recommendations of this report.

The FBI's Implementation of CALEA

Enacted in 1994 at the beginning of the rise in wireless telecommunications, the *Communications Assistance for Law Enforcement Act* (CALEA) sought to help law enforcement agencies continue to conduct electronic surveillance amid changing technology. CALEA requires telecommunications carriers to modify their services and equipment to accommodate law enforcement's need to perform electronic surveillance. The legislation appropriated \$500 million to reimburse carriers for their costs.

A review by the OIG's Audit Division found that CALEA implementation has faced several challenges since its enactment over a decade ago. The most formidable challenge has been the rapid growth of new technologies, such as Internet telecommunications and wireless communications, and whether these new technologies fall under the legislation. After 10 years and over \$450 million invested, the FBI estimates that only 10 to 20 percent of the wireline switches (a telephone company device that "makes the connection" when a call is placed) and approximately 50 percent of the pre-1995 and 90 percent of the post-1995

wireless switches, respectively, have CALEA software activated.

Delays in CALEA implementation have been due in large part to the time consuming development of electronic surveillance standards and extended negotiations over software activation agreements. Initial CALEA standards took 10 years to develop and implement because of litigation. However, litigation regarding CALEA continues today. In addition, the FBI has ongoing negotiations with two wireline carriers to deploy CALEA software on pre-1995 wireline equipment. According to law enforcement officials, technological innovation and time delays in implementing CALEA software have significantly handicapped their efforts to conduct wiretaps. Without changes in existing CALEA requirements and how the FBI exercises its responsibilities, the OIG concluded that the goals envisioned by Congress in 1994 will not be achieved.

We made 6 recommendations regarding the FBI's responsibility for CALEA implementation, including improving communications between law enforcement and carrier representatives, collecting and monitoring data regarding CALEA compliance, and revisiting current plans for the remaining \$45 million in CALEA funding. The FBI concurred with all of our recommendations.

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. We also evaluated the accuracy and appropriateness of the data that participating federal, state, and local laboratories have submitted to the FBI. Below are two examples of findings reported in our audits:

- ◆ The State of Iowa Criminalistics Laboratory in Ankeny, Iowa, was not in compliance with all the standards governing CODIS activities for the areas we tested. The Laboratory did not meet NDIS participation requirements because it did not: 1) ensure that all CODIS users certified annually were aware of and familiar with the requirements, and 2) maintain documentation showing that NDIS candidate matches were addressed in a timely manner. In addition, we found that the Laboratory uploaded one DNA profile that was not allowed for inclusion in NDIS. The Laboratory has since taken the necessary steps to remove the unallowable profile from CODIS and has improved its controls to ensure compliance with NDIS participation requirements.
- ◆ The State of Mississippi Department of Public Safety, Mississippi Crime Laboratory in Jackson, Mississippi, was not in compliance with one of the standards governing CODIS activities for the areas we tested. The Laboratory did not confirm the match of 2 NDIS offender match cases within the required 30 days because of limited staffing and casework duties. NDIS operational procedures require that a NDIS offender match be resolved no more than 30 calendar days after a laboratory is notified of the candidate match. We recommended that the FBI ensure that the Laboratory complete match confirmations in a timely manner. The FBI agreed with our recommendation.

Investigations

During this reporting period, the OIG received 671 complaints involving the FBI. The most common allegations made against FBI employees included waste or misuse of government property, job performance failure, and misuse of a credit card. The OIG opened 17 cases and referred 63+ allegations to the FBI's Inspection Division for investigation.

At the close of the reporting period, the OIG had 44 open cases of alleged misconduct against FBI employees. The criminal investigations cover a wide range of offenses, including the improper release of information, theft of government funds, and fraud. The administrative investigations include serious allegations of misconduct and allegations against high-level employees. The following are examples of cases involving the FBI that the OIG's Investigations Division investigated during this reporting period:

- ◆ An investigation by the OIG's Dallas Field Office led to the arrest, plea, and sentencing of an FBI special agent on fraud charges. The investigation determined that the special agent exceeded his authorized access by querying the FBI's Automated Case Support system for information regarding a counterfeit check cashing and identity theft investigation targeting his brother-in-law and providing the information to his brother-in-law. Additionally, the special agent did not disclose his relationship with his brother-in-law to the FBI until after his brother-in-law's arrest. The special agent was ordered to pay a \$5,000 fine and resign from his position pursuant to a plea agreement with the USAO for the Southern District of Texas.

- ◆ A joint investigation by the OIG's New York Field Office and the FBI resulted in the arrest of an FBI special agent on charges of fraud and making false statements. An indictment returned in the Southern District of New York alleged that the special agent submitted false statements in a visa application for a cooperating witness. The special agent also allegedly concealed his intimate relationship with the witness from the FBI and made false assertions concerning the information and value of information she provided. Judicial proceedings continue.

Ongoing Work

Ojeda Rios Shooting

At the request of the FBI Director, the OIG initiated an investigation of an FBI shooting incident in Puerto Rico that resulted in the death of Filiberto Ojeda Rios. Ojeda was a founder and leader of Los Macheteros, a pro-independence organization in Puerto Rico. Ojeda was arrested in 1955 in connection with a major bank robbery in Connecticut, but had been a fugitive since fleeing in 1990 while released on bail. During the FBI's attempt to arrest Ojeda at a rural residence in western Puerto Rico on September 23, 2005, an FBI agent was wounded and Ojeda was shot and killed. The OIG is examining the circumstances surrounding the shooting and the FBI's entry into the residence.

FBI Reports of Alleged Abuse of Military Detainees

The OIG is reviewing FBI employees' observations and actions related to alleged abuse

of detainees at Guantanamo Bay, Iraq, and Afghanistan. The OIG is examining whether FBI employees participated in any incident of detainee abuse in military facilities at these locations, whether FBI employees witnessed incidents of abuse, how FBI employees reported observations of abuse, and how those reports were handled by the FBI and the Department.

The FBI's Handling of Chinese Intelligence Asset Katrina Leung

At the request of the FBI Director, the OIG is reviewing the FBI's performance in connection with the handling of Katrina Leung, an asset in the FBI's Chinese counterintelligence program who had a long-term intimate relationship with her FBI handler, former Special Agent James J. Smith. The OIG is examining a variety of performance and management issues related to the FBI's handling of Leung.

The FBI's Use of Certain Patriot Act Authorities

As required by the *USA Patriot Improvement and Reauthorization Act* of 2005, the OIG is reviewing the FBI's use of authorities modified under the Patriot Act to obtain business records for foreign intelligence purposes and to issue National Security Letters. Our review will examine the effectiveness of these investigative tools and identify any noteworthy circumstances related to their use. We also will examine what information was collected, retained, and analyzed, and how it was used and disseminated; any procedural delays that may have harmed national security; and any impediments that may have prevented the FBI from making full use of the authorities under the Patriot Act.

Follow-up Examining Implementation of Recommendations in the Hanssen Review

The OIG is conducting a 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 Detering, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen." The OIG 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 will assess the FBI's response to recommendations in the report.

Follow-up on the FBI's Control Over Weapons and Laptop Computers

In August 2002, the OIG issued several audit reports on the control of weapons and laptop

computers by various Department components. These reports detailed significant lapses in the control of weapons and laptops, particularly in the FBI. Our follow-up audit will focus on the FBI's efforts to take corrective action on the recommendations in our original audit report.

CODIS Operational and Laboratory Vulnerabilities

As a follow-up to our 2001 report on CODIS, which was described in our September 2001 *Semiannual Report to Congress*, the OIG is analyzing findings from DNA laboratory audits – both OIG-conducted audits and external quality assurance audits – to determine if they reveal global trends and vulnerabilities. We also are assessing the adequacy of the FBI's administration of CODIS, including its oversight of the national DNA database, and evaluating its implementation of corrective actions in response to the original report.

Office of Justice Programs



OJP manages the Department's multi-faceted grant program. Since its inception in 1984, OJP has awarded more than 80,000 grants totaling more than \$39 billion for a wide variety of programs to prevent and control crime. OJP has about 700 employees and is composed of 5 bureaus – BJA, Bureau of Justice Statistics (BJS), 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

Oversight of Department Expenditures Related to Hurricane Katrina

Prior to Hurricane Katrina, BJA awarded 29 Edward Byrne Memorial Justice Assistance Grants (JAG) to state and local governments that were subsequently affected by the hurricane. JAG funds cover additional personnel, equipment, supplies, contractual support, training, technical assistance, and information systems for criminal justice.

After the hurricane, BJA officials looked for additional funds that could be used to assist law enforcement agencies in the affected areas, and identified approximately \$5 million in unobligated funds. After a review of JAG program requirements by OJP's Office of General Counsel, it was determined that the unobligated grant funds identified by BJA could be used for Hurricane Katrina disaster relief. BJA subsequently provided 29 supplemental JAG awards to state and local governments that had existing JAGs prior to Hurricane Katrina, and awarded 4 new grants to state and local governments that previously submitted JAG applications.

The OIG's Audit Division completed a limited scope audit of BJA, in coordination with the President's Council on Integrity and Efficiency, as part of its examination of relief efforts provided by the federal government in the aftermath of Hurricanes Katrina and Rita. We assessed whether BJA followed existing internal control procedures when awarding the Hurricane Katrina disaster relief grants. We concluded that BJA, while proactive in providing additional grant funding to grantees in the Hurricane Katrina affected areas, had no assurance that funding was going to the areas of greatest need.

For future disaster relief funding, we recommended that OJP perform an assessment of potential grantees to ensure that funding is provided to those with the greatest need. OJP agreed with our recommendation.

Forensic Science Improvement Grant Program

The OIG's Evaluation and Inspections Division reviewed the FY 2005 announcement and application review process for the Paul Coverdell Forensic Science Improvement Grants. NIJ,

under OJP's legal and fiscal oversight, distributed \$13.6 million in FY 2005 Coverdell Grants, which provide funding to state and local governments to improve the timeliness and quality of forensic science and medical examiner services and to eliminate backlogs in the analysis of forensic evidence. The OIG evaluation focused particularly on NIJ's implementation of a requirement imposed by the *Justice for All Act of 2004* that grant recipients certify that they have a process in place for independent, external investigations if allegations arise of "serious negligence or misconduct substantially affecting the integrity of the forensic results."

Our review found that NIJ did not enforce the Act's certification requirement. NIJ's FY 2005 Coverdell Grant Program Announcement did not give applicants necessary guidance on what constitutes an independent external investigation or how to make the required certification. In addition, the announcement did not provide examples of external investigation certifications and did not require an applicant to name the government entity responsible for conducting independent, external investigations. NIJ was aware of the shortcomings in the announcement because of questions it received from potential applicants and concerns expressed by the OIG, but failed to correct them.

The lack of guidance in the program announcement and NIJ's response to the applicants' questions about the new requirement resulted in inadequate certifications. As a result, NIJ directed all 223 applicants to complete and submit a re-certification form. However, the re-certification effort again did not provide specific guidance to applicants, and the form did not require applicants to submit the information necessary to evaluate the certification. Consequently, NIJ funded 37 applications containing external investigation certifications that the OIG found were not in the form NIJ prescribed.

The OIG made three recommendations to improve the program announcement and application process. OJP concurred with one recommendation and partially concurred with the other two.

OVC's Tribal Victim Assistance Program

A 2001 study conducted by BJS indicated that Native Americans are more likely to be victims of rape or sexual assault, aggravated assault, and simple assault than people of any other race in the United States. OVC initiated the Tribal Victim Assistance Grant Program to expand and improve direct service victim assistance programs for federally recognized tribes.

The OIG's Audit Division initiated an audit as a follow-up to our March 2005 report on the administration of grants the Department has awarded to Native American Tribal Governments. The follow-up audit evaluated four individual grantee tribal victim assistance programs and the overall effectiveness of OVC's Tribal Victim Assistance Grant Program.

We found a wide range in the effectiveness of the four individual grantee programs audited. For example, we determined that the Sault Ste. Marie Tribe and the Lummi Indian Nation effectively implemented comprehensive victim assistance programs that bridged the gap between the criminal justice system and victims. Conversely, the Oglala Sioux Tribe and the Mississippi Band of Choctaw Indians did not effectively implement comprehensive victim assistance programs. This unevenness resulted, in part, because OVC did not incorporate adequate strategic planning into its Tribal Victim Assistance Grant Program, which was necessary to implement effective performance-based management. We also found that OVC did not establish long-term or annual program goals for its Program.

Our report concluded that OVC program officials and tribal grantees were not held accountable for performance results. There was no guidance from OVC on collecting performance information, nor was there consistency or comparability among tribal grantees in how the data was reported. We provided seven recommendations that focus on establishing annual and long-term performance goals to measure program results and resource allocation decisions.

OVC agreed with all of our recommendations.

OJP Grants to State and Local Entities

The OIG continued to audit grants awarded by OJP. Examples of findings from these audits issued during this reporting period included the following:

- ◆ BJA awarded the City of New York Police Department (NYPD) a grant of nearly \$4 million to provide personal protective equipment kits and related accessories to 9,935 police officers for protection during hazardous materials incidents. Our audit determined that the NYPD was in material noncompliance with grant requirements and, as a result, we questioned the entire grant amount. We found weaknesses in the NYPD's reporting, including inaccurate and missing financial and progress reports, grant expenditures that were unallowable because of an unauthorized sole-source procurement and unsupported because of inadequate documentation, poor internal controls over the authorization and use of grant funds, a lack of written procedures for reporting grant expenditures and performance, and equipment management procedures that did not fully account for physical property. We made 6 recommendations to remedy questioned costs of nearly \$4 million in unsupported

and unallowable expenditures, strengthen procedures for managing grant funded equipment, and improve internal controls over grant administration in general. OJP agreed with our recommendations.

- ◆ BJA awarded 3 Project Safe Neighborhoods grants totaling approximately \$2.8 million to the North Carolina Department of Crime Control and Public Safety. The purpose of the grants was to implement a strategy to reduce gun violence in areas of North Carolina, primarily by providing subgrants to community service organizations and local authorities. We determined that unsupported and unallowable costs were reimbursed to the grantee for some personnel, equipment, training, and indirect expenditures because the state's fiscal agent for the grant did not reconcile subgrantees' claims for reimbursement to supporting documentation. As a result, we questioned \$170,046 of the total grant funds awarded. We made 12 recommendations to ensure that grant reporting requirements are met, the subgrantees' claims against supporting documents are monitored, and questioned costs are remedied. OJP concurred with all of our recommendations.
- ◆ NIJ awarded a Secure Weapons Systems Technology Program grant totaling around \$2.3 million to FN Manufacturing, LLC, in Columbia, South Carolina, between June 2001 and September 2005. The grant was used to research microelectronics to prevent unauthorized users from firing a law enforcement officer's handgun, and to develop and test a prototype "smart" handgun. FN Manufacturing met the first objective but had not completed a working prototype weapon at the time of our audit. We identified \$140,029 in unsupported costs because FN Manufacturing did not exercise adequate management and control over its grant budget. We also determined that FN Manufacturing

did not obligate \$97,143 in grant funds prior to the end date of the grant. As a result, we reported total dollar-related findings of \$237,172. We made 6 recommendations to ensure that grant reporting requirements are met, ensure compliance for budget modifications that exceed 10 percent of the approved budget, and remedy questioned costs. OJP concurred with all our recommendations.

Investigations

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

At the close of the reporting period, the OIG had 19 open cases of alleged misconduct against OJP employees, contractors, or grantees. The most common allegation was grantee fraud. The following are examples of cases involving OJP that the OIG's Investigations Division investigated during this reporting period:

- ◆ An investigation by the Fraud Detection Office led to the indictment of several leaders of a Las Vegas, Nevada, church on charges of conspiracy, mail fraud, wire fraud, theft of government property, false statements, and obstruction of justice. OIG investigators determined that the church leaders – a civilian pastor, his wife, and a civilian reverend – received a \$423,000 BJA grant through the Alliance Collegiums Association of Nevada to fund the creation of a prisoner re-entry program for southern Nevada. Rather than establish the program, the individuals expended more than \$330,000 for personal use, and thereafter created false documents to cover up their activities. The pastor's wife also was charged with bank fraud, identity

theft, bankruptcy fraud, and misuse of a social security number. Judicial proceedings continue.

- ◆ An investigation by the OIG's Fraud Detection Office and the Lansing, Michigan, Police Department resulted in the arrest of a Department grantee on charges of making a false statement and wire fraud. An indictment returned in the Western District of Michigan alleged that, while serving as executive director of the Lansing-based Neighborhood Youth and Parent Prevention Partnership – which is partially funded by OJP grants – the grantee engaged in fraudulent schemes resulting in the theft of over \$100,000 in Department grant funds. In one scheme, the grantee allegedly wrote more than 200 checks for reimbursement of official expenses that were for her personal benefit. Judicial proceedings continue.

Ongoing Work

The National Law Enforcement and Corrections Technology Center System

The National Law Enforcement and Corrections Technology Center (NLECTC) system, comprised of 10 centers nationwide, is operated by NIJ's Office of Science and Technology (OST). Most NLECTC activities involve anti-crime technologies used by state and local law enforcement agencies and the correctional community to respond to terrorism attacks, major accidents, natural disasters, and threats to school safety. The OIG is evaluating program oversight by NIJ and OST and the effectiveness of the individual sites and the center system as a whole. We also are reviewing NLECTC's efforts to meet the goals set forth in the *Homeland Security Act of 2002*, and are examining program activity levels of the individual centers to determine if funding is adequate and how award funds are being spent.

Bureau of Alcohol, Tobacco, Firearms and Explosives



ATF's more than 5,000 employees perform the dual responsibilities of enforcing federal criminal laws and regulating the firearms and explosives industries. ATF works to investigate and reduce violent crime involving firearms and explosives, acts of arson, and illegal trafficking of alcohol and tobacco products. ATF provides training and support to its federal, state, local, and international law enforcement partners, and works primarily in 23 field divisions across the 50 states, Puerto Rico, the U.S. Virgin Islands, and Guam. Foreign offices are located in Mexico, Canada, Colombia, and France.

Reports Issued

Follow-up of ATF's Forensic Science Laboratories Workload

ATF operates three regional forensic science laboratories to support the enforcement of laws related to firearms, explosives, arson, alcohol, and tobacco. The laboratories also support regulatory functions associated with the firearms and explosives industries. Laboratory staff examine firearms, toolmarks, fire debris, explosives materials, latent prints, documents, and trace evidence. In addition, ATF forensic examiners provide training, crime scene assistance, and court testimony. In FY 2005, ATF laboratories performed over 2,600 forensic examinations with an authorized staff of 106 positions and a budget of approximately \$16 million.

The OIG's Audit Division evaluated whether the laboratories managed workloads effectively to pro-

vide timely services to ATF field divisions. This audit followed up on findings reported in 2001 by the Department of Treasury OIG – which was responsible for auditing ATF until its transfer to the Department in 2003 – that the laboratories did not always provide timely service and did not properly prioritize workloads.

Our audit found that processing times have not significantly improved in the past 4 years. Two-thirds of completed forensic examinations continued to take more than 30 days to complete and about one-third of examinations took more than 90 days. Although customers appreciated the quality of work the laboratories produced, more than half the special agents we interviewed said they used other laboratories at times to obtain more timely results.

Improvements in the timeliness of laboratory examinations have been limited because ATF

has not accomplished actions it committed to in 2001, such as increasing the number of examiner positions in the forensic laboratories, implementing a new priority system, implementing a new information management system, and significantly reducing the size of its backlog of examination requests. Laboratory staffing generally was adequate to manage the incoming workload, but backlogged requests continued to interfere with the timely analysis of incoming examination requests.

The audit found that the backlog could increase as a result of unusually resource-intensive cases. We concluded that if these conditions are not addressed serious consequences may result, such as delays in making arrests and bringing offenders to trial.

In our report, we recommended that ATF develop and implement plans to: 1) eliminate the backlog in each regional forensic science laboratory; 2) manage unusually high incoming workloads that are associated with resource-intensive cases; 3) form agreements and contracts with other laboratories to perform forensic work to provide support when the demand for examinations is unusually high and to help eliminate the backlog; 4) prioritize all incoming evidence submissions to support its investigative priorities and establish realistic time standards for completion; 5) ensure that special agents are educated on the new priority system and comply with its requirements; and 6) reduce the time it takes to fill examiner vacancies.

ATF concurred with our recommendations and indicated that it was in the process of taking corrective action.

Investigations

During this reporting period, the OIG received 202 complaints involving ATF. The most common allegations made against ATF employees included waste, misuse of government property, and job performance failure. The OIG opened 3 investigations and referred 197 allegations to ATF's Office of Professional Responsibility and Security Operations, Investigations Division.

At the close of the reporting period, the OIG had four open cases of alleged misconduct against ATF employees. The allegations included release of information, job performance failure, and misuse of a government-owned vehicle. The following are examples of cases involving ATF that the OIG's Investigations Division investigated during this reporting period:

- ◆ An investigation by the OIG's Detroit Area Office led to the arrest of an ATF special agent on charges of computer fraud. OIG investigators developed evidence that the special agent accessed law enforcement databases to run unauthorized inquiries relating to a convicted drug dealer with whom she had a romantic relationship. The special agent has since left her position with ATF. Judicial proceedings continue.
- ◆ An investigation by the OIG's Philadelphia Area Office and ATF's Office of Professional Responsibility led to the arrest and guilty plea of an ATF special agent, who served as the New York Metropolitan Regional Coordinator for the Organized Crime and Drug Enforcement Task Force, to charges of

theft of government funds. The investigation developed evidence that the special agent fraudulently collected a government salary for hours he spent managing a company he owned in Perth Amboy, New Jersey. Sentencing is pending.

Ongoing Work

Violent Crime Impact Teams

The OIG is evaluating an ATF initiative, Violent Crime Impact Teams, which is intended to reduce violent firearms crimes in select cities across the United States. This review will assess whether ATF effectively implemented the Violent Crime Impact Teams and whether the teams are achieving the program's stated goal of reducing violent crime.

Management of Seized Assets by ATF

Federal statutes authorize law enforcement agencies to seize assets associated with suspected criminal activity. ATF special agents seize property such as firearms, explosives, ammunition, vehicles, and monetary instruments for use as evidence during criminal investigations. This property must be inventoried, stored, and safeguarded pending the outcome of a criminal investigation. The OIG is assessing ATF's management of seized assets by examining its compliance with applicable federal laws, regulations, and Department policies and procedures that apply to seized assets; assessing the adequacy of its controls over accounting for, storing, and safeguarding seized assets in its possession; and analyzing ATF's accounting for the disposition of its seized assets.

Federal Bureau of Prisons



Reports Issued

The BOP's Pharmacy Services

The BOP is faced with a significant challenge to provide adequate and cost-effective medical care to inmates. The BOP's total health care costs for treating inmates increased from approximately \$413 million in FY 2000 to approximately \$624 million in FY 2004, an average annual increase of close to 11 percent. During that same period, the BOP's costs for prescription medications and related supplies increased an average of 23 percent annually, from \$22.5 million in FY 2000 to \$50.7 million in FY 2004.

The OIG's Audit Division evaluated the BOP's efforts to reduce the increasing costs of prescription medications, and assessed whether the BOP ensures adequate controls and safeguards over prescription medications. We concluded that the BOP could reduce prescription medication costs associated with waste from unused prescriptions, which totaled an estimated \$2.81 million in FY 2004. The BOP also should

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 35,000 employees and operates 113 institutions, 6 regional offices, and 2 staff training centers. The BOP is responsible for the custody and care of approximately 189,000 federal offenders, 161,000 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.

ensure that cost-savings initiatives, such as requiring inmates to pay for over-the-counter medications, are fully implemented. In addition, we identified errors related to the controlled substances inventory and administration records. For example, the 12 BOP institutions included in our audit could not account for 402 doses of controlled substances that should have been on hand at the time of our review.

Our audit also concluded that the BOP's plan to implement "Central Fill," through which the Department of Veterans Affairs will fill certain prescriptions at a central location and mail those prescriptions overnight to BOP institutions, will not result in a savings of \$1.14 million per year – as estimated by the BOP – but actually cost the BOP as much as \$895,000 more per year.

Our report contained 13 recommendations for the BOP to improve the administration of its Pharmacy Services. The BOP concurred with the recommendations.

Investigations

During this reporting period, the OIG received 2,552 complaints involving the BOP. The most common allegations made against BOP employees included job performance failure and other official misconduct, use of unnecessary force and other rights violations, and off-duty misconduct. The vast majority of complaints dealt with non-criminal issues that the OIG referred to the BOP's Office of Internal Affairs.

At the close of the reporting period, the OIG had 227 open cases of alleged misconduct against BOP employees. The criminal investigations cover a wide range of allegations, including bribery, introduction of contraband, and sexual abuse of an inmate. The following are examples of cases involving the BOP that the OIG's Investigations Division investigated during this reporting period:

- ◆ An investigation by the OIG's Philadelphia Area Office led to the arrest and guilty plea of a BOP senior correctional officer assigned to the Federal Detention Center (FDC) in Philadelphia, Pennsylvania, to charges of bribery. The OIG investigation determined that the officer procured cell phones, drugs, and other contraband for several prisoners in exchange for bribe payments in excess of \$12,000. The officer was sentenced to 1 year incarceration and 3 years' supervised release, and ordered to pay a \$15,000 fine.
- ◆ An investigation by the OIG's Washington Field Office led to the arrest of a BOP utility system supervisor assigned to the Federal Prison Camp in Alderson, West Virginia, on charges of sexual abuse of a ward. OIG investigators developed evidence that the utility supervisor had a sexual relationship

with an inmate. He was sentenced to 6 months' incarceration and ordered to pay a \$1,000 special assessment to the BOP inmate relief fund and register as a sex offender.

- ◆ An investigation by the OIG's Houston Area Office led to the arrest of a BOP correctional officer assigned to the U.S. Penitentiary in Pollock, Louisiana, on charges of bribery, possession with intent to distribute a controlled substance, and providing or possessing contraband. During the investigation, the correctional officer met with an OIG undercover agent and accepted jewelry and approximately 1 pound of marijuana. The correctional officer also accepted a \$1,000 monetary bribe to introduce contraband for an inmate at the penitentiary. Judicial proceedings continue.
- ◆ An investigation by the OIG's Denver Field Office led to the arrest of a BOP teacher, assigned to the Federal Correctional Institution in Florence, Colorado, on charges of sexual abuse of a ward. OIG investigators developed evidence that the teacher was involved in a sexual relationship with an inmate who was the leader of a prison gang. When interviewed, she admitted to having sex with the inmate on 10 occasions. Judicial proceedings continue.
- ◆ A joint investigation by the OIG's San Francisco Area Office and the FBI's Honolulu Office led to the arrest of a BOP correctional officer assigned to the FDC in Honolulu, Hawaii, on charges of providing contraband to an inmate. The officer confessed to investigators that on at least four occasions he accepted money to introduce methamphetamine and marijuana into the FDC. Judicial proceedings continue.

- ◆ A joint investigation by the OIG's Los Angeles Field Office and the FBI led to the arrest of three BOP correctional officers and one former BOP correctional officer, currently employed as an U.S. Immigration and Customs Enforcement (ICE) agent by the DHS, on charges of bribery. The OIG investigation revealed that the correctional officers accepted cash bribes in return for delivering cellular phones and cigarettes to inmates at the Metropolitan Detention Center in Los Angeles, California. Judicial proceedings continue.

Ongoing Work

Controls Over Inmate Mail

Three terrorists convicted of the 1993 bombing of the World Trade Center allegedly wrote approximately 90 letters while incarcerated in federal prison to Islamic extremists in other countries, including inmates who had been part of a Spanish terror cell tied to the 2004 Madrid terrorism attacks. The letters, which praised Usama Bin Laden, were printed in Arabic newspapers and used to recruit other terrorists. As a result, the OIG is assessing the BOP's inmate mail screening and translation procedures to determine whether the BOP ensures that federal inmates are not using the mail system or the cover of a foreign language to continue criminal behavior, encourage the furtherance of criminal behavior, or encourage any activity that may threaten the public or national security.

U.S. Marshals Service



Reports Issued

USMS Intergovernmental Service Agreements for Detention Facilities

The USMS houses more than 47,000 detainees throughout the nation and is responsible for their transportation from the time they are brought into federal custody until they either are acquitted or incarcerated. To house the detainees, the USMS executes contracts known as Intergovernmental Service Agreements (IGA) with state and local governments to rent jail space. According to the USMS, 75 percent of the detainees in USMS custody are detained in state, local, and private facilities.

During this reporting period, we completed audits of two high-dollar IGAs that the USMS awarded to local governments for the housing and transportation of federal detainees. Our audits found:

- ◆ The USMS awarded an IGA to the Western Tidewater Regional Jail (WTRJ) in Virginia for the housing and transportation of federal

The USMS protects more than 2,000 federal judges and other members of the federal judiciary, transports federal prisoners, protects endangered federal witnesses, manages assets seized from criminal enterprises, and pursues and arrests federal fugitives. 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.

detainees. Our audit determined that the USMS overpaid the WTRJ by \$2.9 million for FYs 2004 and 2005. Additionally, we determined that the USMS could have saved \$1.6 million by implementing the audited rate for FY 2006. We found that the overpayments primarily were due to the USMS awarding the WTRJ a \$65 jail day rate even though WTRJ's unaudited cost sheet only supported a \$52.26 jail day rate.

- ◆ The USMS awarded an IGA to the Doña Ana County Detention Center in New Mexico for the housing and transportation of federal detainees. Our audit determined that the Detention Center's allowable costs did not support the jail daily rate paid by the USMS for FYs 2003 and 2004. During this period, the USMS could have saved more than \$5.2 million by paying the audit calculated rate instead of the rate it agreed to. In addition, the USMS could save more than \$3.2 million annually by paying the audit calculated rate for future fiscal years.

Ongoing Work

The USMS's Justice Prisoner and Alien Transportation System

The Justice Prisoner and Alien Transportation System (JPATS) transfers prisoners and aliens in federal custody within the United States and overseas; performs scheduling, security, and medical functions in support of prisoner

transportation; and provides air transportation for the USMS's Witness Security Program and for federal government responses to crises such as the September 11, 2001, terrorism attacks and the hurricanes of 2005. Managed by the USMS, JPATS serves the BOP, USMS, ICE, military, and state and local law enforcement organizations. The OIG is evaluating the USMS's coordination with other agencies regarding the movement of prisoners and aliens, and its ability to effectively manage the risks inherent in prisoner movement to ensure safe and efficient transport.

Drug Enforcement Administration



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

Investigations

During this reporting period, the OIG received 163 complaints involving the DEA. The most common allegations made against DEA employees included job performance failure, release of information, and misuse of a credit card. The OIG opened 10 investigations and referred 147 allegations to the DEA's Office of Professional Responsibility for investigation.

At the close of the reporting period, the OIG had 27 open cases of alleged misconduct against DEA employees. The most common allegations were fraud and theft. 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 Miami Field Office led to the arrest of a DEA special agent on charges of converting property of another, embezzlement of public funds, and money laundering. An indictment returned in the Northern District of Georgia alleged that the special agent, who served as a team leader and evidence custodian at the DEA's Atlanta Airport Task Force from early 2003 to January 2005,

embezzled cash seized from money couriers for drug organizations by instructing local police officers to turn over seized money to him without counting it. The special agent allegedly stole more than \$200,000, and used a portion of the embezzled money to build a custom home in Orlando, Florida. Judicial proceedings continue.

- ◆ An investigation by the OIG's New York Field Office led to the criminal convictions of a DEA contractor and one of its employees on charges of bid rigging. The investigation determined that the employee and his employer submitted three bids – the company's bid of \$18,500 and two forged bids in the amounts of \$25,800 and \$24,000 – to perform electrical work for the DEA. By offering the lowest bid, the company was awarded the contract. With the assistance of the OIG's Fraud Detection Office, the contracting company was debarred from all government contracts until August 2006, while the employee was debarred until August 2008.
- ◆ An investigation by the OIG's Miami Field Office led to the arrest and guilty plea of a DEA supervisory special agent (SSA) on

charges of making false entries and reports of money. Between May 1997 and November 2002, the SSA was responsible for enlisting the assistance of local law enforcement officers to support the mission of the DEA's Caribbean Field Office and for the distribution and funding of local law enforcement officers. OIG investigators developed evidence that the SSA forged the names of local law enforcement officers and subordinate DEA personnel on cash receipt forms to fraudulently claim reimbursement for approximately \$10,000. He was sentenced to 4 years' probation and 6 months' home confinement, and was ordered to pay \$10,001 in restitution.

- ◆ A joint investigation by the OIG's Miami Field Office and the DEA's Office of Professional Responsibility led to the arrest of a DEA special agent in the Southern District of Florida on charges of theft of government funds and making false, fictitious, and fraudulent claims. OIG investigators obtained evidence that the special agent, who previously was assigned to the Miami Field Division, submitted numerous false expense vouchers to the DEA for various career fairs from October 2003 to March 2004 that he did not attend. Based on the special agent's false reimbursement claims, the DEA paid him \$13,405 for expenses that he was not entitled to receive. Judicial proceedings continue.
- ◆ An investigation by the OIG's Miami Field Office led to the guilty plea of a DEA imprest fund custodian, previously assigned to the Nassau, Bahamas, Country Office, to charges of theft of government funds. The OIG developed evidence that the imprest fund custodian stole \$1,836 from the imprest fund and used it to pay a personal debt. Pursuant to her guilty plea agreement, the custodian paid \$1,836 in restitution, was sentenced to 2 years' probation, and fined \$1,000.

Ongoing Work

The DEA's Drug Diversion Program

The OIG is conducting a follow-up review of the DEA's efforts to reduce the diversion of controlled pharmaceuticals. This review will assess the DEA's response to the recommendations made in our October 2002 review as well as the DEA's response to emerging diversion threats, such as illicit Internet pharmacies.

DEA Cash Seizures

In carrying out its mission as the agency responsible for enforcing the controlled substances laws and regulations of the United States, the DEA seizes cash assets that can be traceable to, or intended to be used for, illicit drug trafficking. The OIG is assessing whether the DEA complies with requirements that govern the handling of cash from seizure through distribution.

The DEA's International Operations

Cooperation with foreign law enforcement agencies is essential to the DEA's mission. To support international investigations, the DEA operates 86 offices in 62 foreign countries and assists its foreign counterparts through such activities as bilateral investigations, international forums, and training foreign law enforcement at its facilities in Quantico, Virginia, as well as in the host countries. The OIG is reviewing the staffing and funding of DEA foreign operations and activities, assessing management controls over DEA international enforcement activities and offices, evaluating the exchange of information with foreign governments and the security over the information shared, and examining the outcomes and accomplishments of DEA foreign operations.

Other Department Components

Office of Community Oriented Policing Services

Reports Issued

COPS Methamphetamine Initiative

The OIG's Audit Division examined COPS' administration of the Department's grant program to stem the production, distribution, and use of methamphetamine. Over the past 8 years, Congress has appropriated more than \$200 million for grants to state and local law enforcement agencies to combat methamphetamine. The OIG review found significant deficiencies in COPS' administration of the methamphetamine grant program, in its monitoring of grantee activities, and in the way individual grantees administered their grants.

Between FYs 1998 and 2005, Congress appropriated \$385.6 million for the Methamphetamine Initiative. Of this total, COPS transferred almost \$125 million to the

COPS was created as a result of the *Violent Crime Control and Law Enforcement Act of 1994* to advance community policing in jurisdictions of all sizes across the country. COPS provides grants to tribal, state, and local law enforcement agencies to hire and train community policing professionals, acquire and deploy crime-fighting technologies, and develop and test innovative policing strategies.

DEA for the removal and disposal of hazardous materials from clandestine methamphetamine laboratories, reimbursed OJP \$16.6 million for several Methamphetamine Initiative grants it administered on behalf of COPS, and distributed the balance of \$214 million to state and local entities through the grant process. More than 84 percent (\$179 million) of the state and local grant funds distributed by COPS were earmarks under which Congress designated that a specific project or entity should receive the funds.

The OIG audit found weaknesses in COPS' management and administrative controls related to the Methamphetamine Initiative. Specifically, we identified a lack of coordination between COPS officials, weaknesses in the database that COPS uses to manage and track grants, and insufficient and inconsistent monitoring of

grantees. For example, since FY 1998 only 15 of the 179 Methamphetamine Initiative grantees have received an on-site visit by COPS.

Since FY 2002, the congressional earmarks have included an instruction for COPS to scrutinize the proposed projects, consult with the DEA, and award the funds if warranted. However, we found that COPS has not consulted with the DEA about potential grants before awarding the earmarked funds. Furthermore, while some states with high numbers of reported methamphetamine incidents received significant funds through the Methamphetamine Initiative, other states with similar levels of reported methamphetamine incidents received lower levels of funding.

In addition to examining the overall administration of the methamphetamine grant program, OIG audits of 44 individual state and local grants – totaling more than \$56 million awarded to 13 grantees – identified \$9.5 million in questioned costs and numerous accounting and internal control weaknesses. Our report contained 17 recommendations that focus on specific steps COPS should take to improve the management and administration of the Methamphetamine Initiative, including implementing procedures for the administration and oversight of entities receiving funding as well as evaluating the effectiveness of the grant program as a whole.

COPS Methamphetamine Grants to State and Local Entities

The OIG completed several audits of methamphetamine grants awarded by COPS. Examples of findings from these audits issued during this reporting period included the following:

- ◆ The Pierce County Alliance in Washington State was awarded 3 COPS grants totaling nearly \$9 million to assist state and local

law enforcement agencies in reducing the production, distribution, and use of methamphetamine. We determined that the Alliance had not followed grant requirements concerning the hiring and billing of sheriffs' deputies. We also found that the Alliance could not provide documentation disputing the notion that grant funds were used to supplant local budgets. In addition, the Alliance could not provide adequate supporting documentation for non-personnel expenditures that were charged to the grants. As a result, we reported total questioned costs of \$2.4 million and recommended that COPS remedy these questioned costs. COPS concurred with our recommendation.

- ◆ The Mississippi Bureau of Narcotics (MBN) in Jackson, Mississippi, was awarded 4 grants totaling over \$2.6 million for the COPS Methamphetamine Initiative. We found that MBN's accounting systems and procedures did not accurately account for grant funds disbursed, which made it impossible to reconcile grant drawdowns with accounting system reports or other accounting records. Therefore, we questioned as unsupported the total amount of nearly \$2 million drawn down by MBN. We also determined that MBN had not expended \$98,127 of the funds awarded for closed grants, which should be deobligated and put to better use. In addition, we identified deficiencies in the areas of budget management and control, grant expenditures, and reporting. We recommended that COPS remedy questioned costs; deobligate unneeded grant funds; and ensure that grant reporting requirements are met, disbursements of grant funds are properly accounted, and property is accurately recorded. COPS concurred with all of our recommendations.
- ◆ COPS awarded 4 grants totaling nearly \$2.4 million to the Vermont State Police (VSP) under the Methamphetamine Initiative. The grants were used to fund personnel, sup-

plies, and other expenses intended to reduce the production, distribution, use, and associated crime of heroin and methamphetamine. Funds also were used to train police officers and provide community education outreach on the methamphetamine problem. We questioned costs of just over \$1.2 million, or nearly 50 percent of the total funding, for all 4 grants after determining that VSP was reimbursed nearly \$1.2 million for law enforcement salary and fringe benefit expenditures prohibited by the guidelines covering these grants. We also found that unallowable costs were included in VSP grant budgets approved by COPS. Further, VSP charged the grants \$27,174 for

personnel, supplies, and administrative expenses that were unallowable because COPS had not approved the expenditures. Because VSP did not collect relevant data and develop performance measures, it was unable to determine the overall effect the grants were having on reducing heroin and methamphetamine use and related crime throughout the state. We made 8 recommendations to remedy questioned costs of nearly \$1.2 million in unallowable expenditures and supplanted local funds, implement a performance measurement process to assess accomplishments, and strengthen budget procedures. COPS concurred with all of our recommendations.

outdated and disorganized. Further, analytical products developed by the specialists were not consistently reviewed or widely disseminated within the Department.

The OIG made eight recommendations to the EOUSA to improve the USAOs' use of intelligence research specialists, including: 1) identify and provide the standard tools specialists need, define the types of work products specialists should produce, and establish quality standards for those products; 2) provide specialists with current and complete policy guidance; 3) survey users of specialists' work to ascertain its applicability and quality and identify areas for improvement; and 4) reassess the specialists' role and duties in light of the pending reorganization of the Department's intelligence activities.

The EOUSA concurred with all of our recommendations.

Investigations

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

- ◇ An investigation by the OIG's Los Angeles Field Office led to the arrest and guilty plea to charges of wire fraud of a civilian assigned to the Xerox contract with the USAO for the Central District of California. The OIG investigation revealed that the Xerox employee ordered toner and other printing supplies under the guise of the Department's fixed price contract, then stole approximately \$730,000 in the merchandise from the U.S. Courthouse for the Central District of California in a 10-month period and sold the merchandise for his own profit. The Xerox employee was sentenced to 6 months' home confinement and 5 years' supervised release, and ordered to pay \$40,000 in restitution.

U.S. Attorneys' Offices

Reports Issued

USAO Intelligence Research Specialists

USAO intelligence research specialists coordinate antiterrorism activities, analyze the relevance and reliability of threat information and investigative leads, and seek to ensure that cases with terrorism connections are identified for prosecution. Each USAO was allocated at least one intelligence research specialist after the September 11, 2001, terrorism attacks.

The OIG's Evaluation and Inspections Division reviewed the role and functions of USAO

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, the U.S. Virgin Islands, Guam, and the Northern Mariana Islands. More than 11,700 employees work in those offices and in the EOUSA.

intelligence research specialists and found that individually the specialists made valuable contributions to the USAOs' antiterrorism efforts. However, their overall effectiveness could be increased through improved coordination and guidance at the regional and Departmental levels. For example, the specialists' efforts to collect intelligence information related to antiterrorism cases and the work products they produced differed markedly from USAO to USAO, making it more difficult for users to identify and act on the intelligence the products conveyed. In addition, the specialists relied on policy guidance that was

Top Management Challenges

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

The OIG's top challenges for this year, issued in October 2005, are listed to the right. The challenges are not presented in order of priority – we believe that all are critical management 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.

Eight of the challenges from last year's list remain and are long-standing, difficult challenges that will not be solved quickly or easily. However, two challenges from last year's list have been replaced by two other challenges. We removed "Human Capital" and "Forensic Laboratories" this year and added two new challenges: "Department and FBI Intelligence-Related Reorganizations" and "Judicial Security."

Top Management and Performance Challenges in the Department of Justice - 2005

1. Counterterrorism
2. Sharing of Law Enforcement and Intelligence Information
3. Department and FBI Intelligence-Related Reorganizations
4. Information Technology Systems Planning and Implementation
5. Information Technology Security
6. Financial Management and Systems
7. Grant Management
8. Detention and Incarceration
9. Judicial Security
10. Supply and Demand for Drugs

Detailed information about these management challenges can be found at www.usdoj.gov/oig/challenges/index.htm.

Congressional Testimony

On October 31, 2005, a director in the OIG's Evaluation and Inspections Division testified before the House Committee on Government Reform, Subcommittee on National Security, Emerging Threats and International Relations, at a field hearing that examined the safeguarding of stored explosives. The director discussed the OIG's review of ATF's implementation of the *Safe Explosives Act*.

On February 14, 2006, the Inspector General testified before the House Committee on Government Reform, Subcommittee on National Security, Emerging Threats and International Relations, at a hearing that examined existing procedures for national security whistleblowers. The Inspector General's testimony related to the OIG's role in investigating whistleblower complaints at the FBI.

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, Congress supported legislation in the *Violence Against Women and Department of Justice Reauthorization Act of 2005* that included recommendations from an April 2005 OIG report entitled, "Deterring Staff Sexual Abuse of Federal Inmates." The legislation increases the statutory penalties that apply to sexual abuse of federal inmates by correctional staff, expands federal jurisdiction to cover sexual abuse of federal inmates confined in non-federal facilities, and expands federal jurisdiction to cover introduction of contraband in state, local, or contract facilities housing federal inmates. The OIG concluded in its report that the federal law then in place was insufficient for deterring sexual abuse at federal correctional facilities because only misdemeanor penalties applied to

sexual abuse or sexual contact of an inmate without the use of force or overt threats. The report also noted a deficiency in the federal law because it did not apply to either staff sexual abuse of inmates or the introduction of contraband into correctional facilities by staff or inmates when those crimes occurred in facilities under contract to the federal government rather than in BOP facilities.

In addition, the OIG reviewed legislation on proposed changes to the whistleblower regulations in 28 C.F.R. Part 27, which govern the process designed to protect FBI employees from retaliation for making protected disclosures. The OIG also reviewed a provision in the *Intelligence Authorization Act for Fiscal Year 2006* that would establish an Inspector General for the intelligence community and grant that Inspector General the "final decision" regarding whether the OIG could undertake particular investigations, audits, or inspections involving certain FBI programs or personnel.

Other legislation reviewed by the OIG during this reporting period included the *Fiscal Year 2006 Department of Justice Appropriations Conference Report* and the *USA Patriot Improvement and Reauthorization Act of 2005*.

Statistical Information

Audit Statistics

Audit Summary

During this reporting period, the Audit Division issued 89 audit reports containing more than \$31 million in questioned costs and more than \$50 million in funds to be put to better use, and made 351 recommendations for management improvement. Specifically, the Audit Division

issued 26 internal reports of Department programs funded at more than \$214 million; 28 external reports of contracts, grants, and other agreements funded at more than \$146 million; and 35 *Single Audit Act* audits. In addition, the Audit Division issued one Notification of Irregularity, and two Management Improvement Memoranda.

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	3	\$2,149,163
Issued during period	8	\$50,478,161
Needing management decision during period	11	\$52,627,324
Management decisions made during period:		
◆ Amounts management agreed to put to better use ¹	7	\$45,757,040
◆ Amounts management disagreed to put to better use	0	\$0
No management decision at end of period	4	\$6,870,284

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

Audits With Questioned Costs			
Audit Reports	Number of Audit Reports	Total Questioned Costs (including unsupported costs)	Unsupported Costs
No management decision made by beginning of period	9	\$6,126,975	\$1,594,205
Issued during period	24	\$31,544,631	\$6,724,661
Needing management decision during period	33	\$37,671,606	\$8,318,866
Management decisions made during period:			
◆ Amount of disallowed costs ¹	24	\$24,599,464	\$6,825,385
◆ Amount of costs not disallowed	0	\$0	\$0
No management decision at end of period	9	\$13,072,142	\$1,493,481

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

Audits 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	7	12
Issued during period	78	351
Needing management decision during period	85	363
Management decisions made during period:		
◆ Number management agreed to implement ¹	78 ²	333
◆ Number management disagreed with	0	0
No management decision at end of period	10	30

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

Audit Follow-Up

OMB Circular A-50

OMB Circular A-50, *Audit Follow-Up*, requires audit reports to be resolved within 6 months of the audit report issuance date. Audit monitors the status of open audit reports to track the audit resolution and closure process. As of March 31, 2006, the OIG had closed 130 audit reports and was monitoring the resolution process of 340 open audit reports.

Unresolved Audits

Audits Over 6 Months Old Without Management Decisions

As of March 31, 2006, the following audits had no management decision or were in disagreement:

- ◇ COPS Grants to the Albuquerque, New Mexico, Police Department
- ◇ COPS Grants to the Picuris Pueblo, New Mexico, Police Department
- ◇ COPS Grants to the Blackfeet Tribal Business Council, Montana
- ◇ COPS Grants to the Navajo Department of Resource Environment, Window Rock, Arizona
- ◇ COPS Grants to the AMTRAK Police Department

- ◇ 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 Blount County, Tennessee, Sheriff's Office

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, 2006.

E&I Workload Accomplishments	Number of Reviews
Reviews active at beginning of period	7
Reviews initiated	5
Final reports issued	3
Reviews active at end of reporting period	9

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, 2006, there are 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, 2006.

Source of Allegations	
Hotline (telephone and mail)	533
Other sources	3,555
Total allegations received	4,088
Investigative Caseload	
Investigations opened this period	185
Investigations closed this period	211
Investigations in progress as of 3/31/06	383
Prosecutive Actions	
Criminal indictments/informations	52
Arrests	48
Convictions/Pleas	47
Administrative Actions	
Terminations	11
Resignations	59
Disciplinary action	10
Monetary Results	
Fines/Restitutions/Recoveries	\$1,828,636
Seizures	\$13,600

Integrity Awareness Briefings

OIG investigators conducted 163 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 8,216 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	FY	Fiscal year
BJA	Bureau of Justice Assistance	ICE	U.S. Immigration and Customs Enforcement
BJS	Bureau of Justice Statistics	IG Act	<i>Inspector General Act of 1978</i> , as amended
BOP	Federal Bureau of Prisons	IT	Information technology
CODIS	Combined DNA Index System	ITIM	Information Technology Investment Management
COPS	Office of Community Oriented Policing Services	NIJ	National Institute of Justice
DEA	Drug Enforcement Administration	OIG	Office of the Inspector General
Department	U.S. Department of Justice	OJP	Office of Justice Programs
DHS	Department of Homeland Security	OMB	Office of Management and Budget
EOUSA	Executive Office for U.S. Attorneys	OVC	Office for Victims of Crime
FBI	Federal Bureau of Investigation	Patriot Act	<i>USA PATRIOT Act</i>
FISA	<i>Foreign Intelligence Surveillance Act</i>	USAO	U.S. Attorneys' Offices
FISMA	<i>Federal Information Security Management Act</i>	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.

Disclaimer of Opinion: A disclaimer of opinion results when auditors are unable to express an opinion on the fairness of the agency's financial statements due to a limiting factor, such as a lack of adequate supporting financial information.

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

Enterprise Architecture: An Enterprise Architecture establishes an agency-wide roadmap to achieve an agency's mission through optimal performance of its core business processes within an efficient IT environment. An Enterprise Architecture is made up of four components: Business Architecture, Applications Architecture, Data Architecture, and Technical Architecture.

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.

Material Weakness: A reportable condition in which the design or operation of the internal control does not reduce to a relatively low level the risk that error, fraud, or noncompliance in amounts that would be material in relation to the principal statements or to performance measures may occur and not be detected within a timely period by employees in the normal course of their assigned duties.

Qualified Opinion: The judgment by the certified public accountant in an audit report that "except for" something, the financial statements fairly present the financial position and operating results of the entity.

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.

Reportable Condition: Includes matters coming to the auditor's attention that, in the auditor's judgment, should be communicated because they represent significant deficiencies in the design or operation of internal controls that could adversely affect the entity's ability to properly report financial data.

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

Unqualified Opinion: An auditor's report that states the financial statements present fairly, in all material respects, the financial position and results of operations of the reporting entity, in conformity with generally accepted accounting principles.

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, 2005 - March 31, 2006

Report to Congress on Implementation
of Section 1001 of the Patriot Act

Review of OJP's Forensic Science
Improvement Grant Program

Review of USAOs' Use of Intelligence
Research Specialists

Appendix 4

Audit Division Reports

October 1, 2005 - March 31, 2006

INTERNAL AND EXTERNAL AUDIT REPORTS

Arkansas National Criminal History Improvement Program Cooperative Agreement Awarded to the Arkansas Crime Information Center

Assets Forfeiture Fund and Seized Asset Deposit Fund Annual Financial Statement for FY 2005

ATF Annual Financial Statement for FY 2005

Compliance with Standards Governing CODIS Activities at the California Department of Justice, Bureau of Forensic Services, Fresno Regional Laboratory, Fresno, California

Compliance with Standards Governing CODIS Activities at the Iowa Criminalistics Laboratory

Compliance with Standards Governing CODIS Activities at the Philadelphia Police Department, Forensic Sciences Division, Philadelphia, Pennsylvania

Compliance with Standards Governing CODIS Activities at the State of Mississippi Department of Public Safety, Mississippi Crime Laboratory

COPS Methamphetamine Grants Awarded to the Mississippi Bureau of Narcotics

COPS Methamphetamine Initiative Grants Administered by the California Department of Justice, Sacramento, California

COPS Methamphetamine Initiative Grants Administered by the Marion County Sheriff's Office, Salem, Oregon

COPS Methamphetamine Initiative Grants Administered by the Pierce County Alliance, Tacoma, Washington

COPS Methamphetamine Initiative Grants Administered by the Vermont State Police

COPS Technology Grants Awarded to Mountain Village, Colorado

DEA Annual Financial Statement for FY 2005

Effectiveness of OVC's Tribal Victim Assistance Program

FBI Annual Financial Statement for FY 2005

FBI's Efforts to Prevent and Respond to Maritime Terrorism

FBI's Implementation of the *Communications Assistance for Law Enforcement Act*

FBI's Pre-Acquisition Planning For and Controls Over the Sentinel Case Management System

BOP Annual Financial Statement for FY 2005

BOP Contract with HCA HealthONE, LLC

BOP Pharmacy Services

Federal Prison Industries, Inc., Annual Financial Statement for FY 2005

Follow-up Audit of ATF's Forensic Science Laboratories Workload Management

Independent Evaluation of the Department's Information Technology Security and Oversight Program Pursuant to FISMA for FY 2004

Independent Evaluation of the Department's Information Security Program and Oversight Pursuant to FISMA for FY 2005

Independent Evaluation of the FBI's Automated Case Support Application System Pursuant to FISMA for FY 2005

Independent Evaluation of the FBI's Information Security Program Pursuant to FISMA for FY 2005

Inventory of Major Department Information System Investments as of FY 2006

COPS Methamphetamine Initiative

OJP Agreement Between the Office of the Police Corps and the Law Enforcement Education and the Massachusetts Criminal Justice Training Council, South Weymouth, Massachusetts

OJP Agreement Between the Office of the Police Corps and the Utah Department of Public Safety, Salt Lake City, Utah

OJP Annual Financial Statement for FY 2005

OJP Beyond Missing Internet Poster Distribution Project, Sausalito, California

OJP Juvenile Accountability Incentive Block Grants to the Oklahoma Office of Juvenile Affairs

OJP National Crime Scene Training Center Cooperative Agreement with the University of New Haven, West Haven, Connecticut

OJP Regional Information Sharing Systems Grants Awarded to the Arizona Department of Public Safety, Rocky Mountain Information Network

OJP BJA Grants Awarded to the North Carolina Department of Crime Control and Public Safety

OJP BJA Safety Equipment Grant to the City of New York Police Department

OJP NIJ Secure Weapons Systems Technology Grant Awarded to FN Manufacturing, LLC

OJP OJJDP Safe Start Demonstration Project Administered by the Chicago Department of Public Health

Offices, Boards and Divisions Annual Financial Statement for FY 2005

Oversight of Department Expenditures Related to Hurricanes Katrina and Rita

Review of the Department's Consolidated Information System General Controls Environment for FY 2005

The Status of Enterprise Architecture and Information Technology Investment Management in the Department

The Department's Annual Financial Statement for FY 2005

USMS Annual Financial Statement for FY 2005

USMS Intergovernmental Service Agreement for Detention Facilities with the Cumberland County Jail, Portland, Maine

USMS Intergovernmental Service Agreement for Detention Facilities with the Western Tidewater Regional Jail, Suffolk, Virginia

USMS Intergovernmental Service Agreement for Detention Facilities with the District of Columbia Department of Corrections

USMS Intergovernmental Service Agreement for Detention Facilities with the Doña Ana County Detention Center, Las Cruces, New Mexico

University of Massachusetts Medical School and Memorial Health Care, Incorporated Compliance with the BOP Contract

Use of Equitable Sharing of Revenues by the Nebraska State Patrol

Working Capital Fund Annual Financial Statement for FY 2005

SINGLE AUDIT ACT REPORTS OF DEPARTMENT OF JUSTICE ACTIVITIES

October 1, 2005 - March 31, 2006

Baltimore County, Maryland

Brazos County, Texas

Catholic Charities of the Diocese of Galveston-Houston, Texas

Choctaw Nation of Oklahoma

City and County of Denver, Colorado

City of Albuquerque, New Mexico

City of Baltimore, Maryland

City of Boca Raton, Florida

City of DeKalb, Texas

City of Little Rock, Arkansas

City of Omaha, Nebraska

City of Tempe, Arizona

City of Tulsa, Oklahoma

Commonwealth of Puerto Rico, Office of Youth Affairs

Commonwealth of Puerto Rico Police

Hall County, Nebraska

Hernando County, Florida

Jonesboro, Arkansas, Police Department

Juvenile Welfare Board, Pinellas County, Florida

Kickapoo Tribe, Kansas

Lincoln County, Montana

Municipality of San Juan, Puerto Rico

National American Indian Court Judges Association, Colorado

Native American Alliance Foundation, Tulsa, Oklahoma

Office of District Attorney, 28th Judicial Circuit, Baldwin County, Alabama

Oklahoma City, Oklahoma

Osage Tribal Council, Pawhuska, Oklahoma

Otoe-Missouria Tribe of Indians, Red Rock, Oklahoma

Parker County, Texas

Pawnee Nation, Pawnee, Oklahoma

Sac and Fox Nation, Stroud, Oklahoma

State of Arkansas

United Keetoowah Band of Cherokee Indians, Oklahoma

University of Arkansas for Medical Sciences

Youth Crime Watch of America, Inc.

Audit Division Reports

October 1, 2005 - March 31, 2006

Quantifiable Potential Monetary Benefits

Audit Report	Questioned Costs	Unsupported Costs	Funds Put to Better Use
Arkansas National Criminal History Improvement Program Cooperative Agreement Awarded to the Arkansas Crime Information Center	\$172,514	\$4,400	
City of Omaha, Nebraska	\$234,401		
Commonwealth of Puerto Rico Police	\$14,116	\$14,116	
COPS Methamphetamine Grants Awarded to the Mississippi Bureau of Narcotics	\$1,968,775	\$1,968,775	\$98,127
COPS Methamphetamine Initiative			\$365,639
COPS Methamphetamine Initiative Grants Administered by the California Department of Justice, Sacramento, California	\$16,575		
COPS Methamphetamine Initiative Grants Administered by the Pierce County Alliance, Tacoma, Washington	\$2,414,098		
COPS Methamphetamine Initiative Grants Administered by the Vermont State Police	\$1,210,767		
COPS Technology Grants Awarded to Mountain Village, Colorado	\$198,817	\$3,240	\$42,807
FBI's Implementation of the <i>Communications Assistance for Law Enforcement Act</i>			\$45,000,000
OJP Agreement Between the Office of the Police Corps and Law Enforcement Education and the Massachusetts Criminal Justice Training Center, South Weymouth, Massachusetts	\$627,849		\$18,595
OJP Agreement Between the Office of the Police Corps and the Utah Department of Public Safety, Salt Lake City, Utah	\$155,066		

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	38
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	6-37
Section 5(a)(2)	Significant Recommendations for Corrective Actions	6-36
Section 5(a)(3)	Prior Significant Recommendations Unimplemented	41-42
Section 5(a)(4)	Matters Referred to Prosecutive Authorities	10, 16-17, 22, 24-25, 27-28, 31-32, 36
Section 5(a)(5)	Refusal to Provide Information	None
Section 5(a)(6)	Listing of Audit Reports	47-51
Section 5(a)(7)	Summary of Significant Reports	6-36
Section 5(a)(8)	Audit Reports – Questioned Costs	40
Section 5(a)(9)	Audit Reports – Funds to Be Put to Better Use	39
Section 5(a)(10)	Prior Audit Reports Unresolved	41
Section 5(a)(11)	Significant Revised Management Decisions	None
Section 5(a)(12)	Significant Management Decisions With Which the OIG Disagreed	None

Audit Report	Questioned Costs	Unsupported Costs	Funds Put to Better Use
OJP Beyond Missing Internet Poster Distribution Project, Sausalito, California	\$17,569	\$13,551	
OJP BJA Grants Awarded to the North Carolina Department of Crime Control and Public Safety	\$170,046	\$166,144	
OJP BJA Safety Equipment Grant to the City of New York Police Department	\$3,974,000	\$3,974,000	
OJP Juvenile Accountability Incentive Block Grants to the Oklahoma Office of Juvenile Affairs	\$10,983,210		
OJP National Crime Scene Training Center Cooperative Agreement with the University of New Haven, West Haven, Connecticut	\$666,360	\$429,300	
OJP NIJ Secure Weapons Systems Technology Grant Awarded to FN Manufacturing, LLC	\$140,029	\$140,029	\$97,143
OJP OJJDP Safe Start Demonstration Project Administered by the Chicago Department of Public Health	\$132,202	\$6,106	
OJP Regional Information Sharing Systems Grants Awarded to the Arizona Department of Public Safety, Rocky Mountain Information Network	\$13,671		
State of Arkansas	\$11,362		
United Keetoowah Band of Cherokee Indians, Oklahoma	\$6,349		
Use of Equitable Sharing of Revenues by the Nebraska State Patrol	\$120,340	\$5,000	
USMS Intergovernmental Service Agreement for Detention Facilities with the Doña Ana County Detention Center, Las Cruces, New Mexico	\$5,231,812		\$3,237,721
USMS Intergovernmental Service Agreement for Detention Facilities with the Western Tidewater Regional Jail, Suffolk, Virginia	\$2,862,349		\$1,618,129
USMS Intergovernmental Service Agreement for Detention Services with the Cumberland County Jail, Portland, Maine	\$202,354		
Total	\$31,544,631	\$6,724,661	\$50,478,161

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 & Civil Liberties Complaints
Office of the Inspector General**

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

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

U.S. DEPARTMENT OF JUSTICE
OFFICE OF THE INSPECTOR GENERAL

ESTABLISHED APRIL 14, 1989