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

Office of the Inspector General Semiannual Report to Congress

October 1, 2007 – March 31, 2008

Online Report Availability

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

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

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

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

Or call: (202) 616-4550

Message From the Inspector General

This semiannual report summarizes the work of the Office of the Inspector General (OIG) from October 1, 2007, through March 31, 2008. OIG staff have continued to conduct valuable audits, inspections, special reviews, and investigations of Department of Justice (Department) programs and operations.

For example, the OIG completed reports evaluating the Federal Bureau of Investigation's (FBI) use of national security letters and Section 215 orders for business records, an audit of the Department's process for nominating known or suspected terrorists to the consolidated terrorist watchlist, an audit of the FBI's management of undercover case funds, an evaluation of the Drug Enforcement Administration's (DEA) controls over its weapons and laptop computers, an audit of the Department's victim notification system, and other important reviews.

In this message, however, I want to highlight the outstanding work of the OIG's Investigations Division, which sometimes does not receive the recognition it deserves. Our experienced investigators continue to handle many significant allegations of criminal and administrative misconduct relating to Department programs, contractors, grants, and employees.

During this 6-month semiannual period, for example, OIG investigators completed 161 investigations, resulting in 56 arrests, 69 convictions, 108 administrative actions, and $4.7 million in civil and administrative recoveries. One of the benefits of an OIG investigation is that it can pursue allegations wherever they lead, whether they result in a criminal action, civil recovery, administrative action, or exoneration.

The OIG handles a wide variety of investigations. Examples include allegations of Federal Bureau of Prisons (BOP) correctional officers smuggling contraband into prison facilities, Department employees' theft of money or property, conflicts of interest, civil rights violations, obstruction of justice, bribery, grant fraud, and violations of other criminal laws and administrative procedures governing Department employees, contractors, and grantees. The cases we discuss in this semiannual report are just a few of the hundreds of matters that our Investigations Division handles at any one time.

One case highlighted in this report concerns an investigation into allegations that correctional officers at the BOP's Metropolitan Detention Center (MDC) in Brooklyn, New York, physically abused inmates and lied about their actions. OIG investigators determined that MDC correctional officers participated in a planned beating of an inmate and then attempted to disguise the attack by planting a noose in the inmate's cell and falsely claiming in written reports that he had become combative when they attempted to prevent him from committing suicide. In a second incident, OIG investigators determined that MDC correctional officers assaulted an inmate in an elevator and then wrote false reports about the attack.

As a result of our investigations, the U.S. Attorneys' Office (USAO) in the Eastern District of New York prosecuted these officers on a variety of charges. Five correctional officers pled guilty, and a BOP captain, BOP lieutenant, and three additional correctional officers were convicted at two trials of charges such as conspiracy to violate the civil rights of an inmate, obstruction of justice, and making false statements. This investigation provides a clear example of the outstanding work of OIG investigators who work hand-in-hand with Department prosecutors to detect and deter misconduct by the relatively small number of Department employees who abuse their authority.

Finally, I want to thank the Department, the new Attorney General, and Congress for their continued support of the work of the OIG. Most important, I want to again thank the dedicated OIG staff who tirelessly perform their mission in an exemplary fashion.

Glenn A. Fine
Inspector General
April 30, 2008

Table of Contents

Highlights of OIG Activities 1

OIG Profile 5

Multicomponent Audits, Reviews, and Investigations 7

Federal Bureau of Investigation 14

Federal Bureau of Prisons 23

Office of Justice Programs 28

Drug Enforcement Administration 33

U.S. Marshals Service 35

Bureau of Alcohol, Tobacco, Firearms and Explosives . . . 36

Other Department Components 37
- U.S. Attorneys' Offices 37
- Executive Office for U.S. Trustees 38
- Criminal Division 39

Top Management and Performance Challenges 40

Congressional Testimony 41

Legislation and Regulations 41

Statistical Information 42
- *Audit Statistics* 42
- Funds Recommended to be Put to Better Use 42
- Questioned Costs 43
- Management Improvements 43
- *National Defense Authorization Act* Reporting 44
- Audit Follow-up 44
- Unresolved Audits 44
- *Evaluation and Inspections Statistics* 45
- *Investigations Statistics* 45

Appendices 46
- Acronyms and Abbreviations 46
- Glossary of Terms 47
- Evaluation and Inspections Division Reports 48
- Audit Division Reports 49
- Reporting Requirements Index 56

Highlights of OIG Activities

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

Statistical Highlights

October 1, 2007 – March 31, 2008

Allegations Received by the Investigations Division	4,630
Investigations Opened	180
Investigations Closed	161
Arrests	56
Indictments/Informations	53
Convictions/Pleas	69
Administrative Actions	108
Fines/Restitutions/Recoveries	$4.7 million
Audit Reports Issued	137
Questioned Costs	$20.8 million
Funds Put to Better Use	$174,000
Recommendations for Management Improvements	322

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

- **The FBI's Use of National Security Letters and Section 215 Authorities.** The OIG issued two follow-up reports in March 2008 evaluating the FBI's use of national security letters (NSL) and Section 215 orders for business records. The NSL report found that the FBI and the Department have made significant progress implementing recommendations in the OIG's first report on NSLs issued the previous year and adopting corrective actions to address the serious problems we identified. We also found that the FBI has devoted substantial time, energy, and resources ensuring that its field managers and agents understood the seriousness of the FBI's shortcomings in its use of NSLs and their responsibility for correcting these deficiencies. With respect to the FBI's use of NSLs, we found a continued upward trend, with more than 49,000 NSL requests issued in 2006. On average, approximately one-third of all counterterrorism, counterintelligence, and cyber investigations that were open at any time during 2006 employed NSLs. The percentage of NSL requests related to investigations of U.S. persons also continued to increase. We also identified NSL-related deficiencies and possible intelligence violations in 2006 similar to the findings in our first report. In our report, we made 17 recommendations to help improve the FBI's use and oversight of NSLs. The FBI agreed with the recommendations and said it would implement additional actions to address our findings.

  With respect to the FBI's use of Section 215 authorities, we found that FBI agents encountered similar processing delays for Section 215 applications in 2006 as those identified in our previous report. Our review did not identify any illegal use of Section 215 orders in 2006, but we found two instances

where the FBI received more information than it requested. We also reported on a case in which the Foreign Intelligence Surveillance Act Court twice refused to authorize a Section 215 order based on concerns that the investigation was premised on protected First Amendment activity. The FBI subsequently issued NSLs to obtain information based on the same factual predicate and without further review to ensure the investigation did not violate the subject's First Amendment rights. In addition, we found that the interim minimization procedures adopted in September 2006 to protect the constitutional rights of U.S. persons do not provide enough specific guidance.

- **The Department's Terrorist Watchlist Nomination Processes.** The OIG examined the Department's processes for nominating known or suspected terrorists to the consolidated terrorist watchlist. We found that while the FBI has developed a formal policy for nominations to the watchlist, no standard nominations policy exists for other Department components that are involved in watchlisting. We also found that FBI case agents did not always update watchlist records when new information became known, and the FBI did not always remove watchlist records when appropriate. Moreover, watchlist nomination submissions from FBI field offices often were incomplete or contained inaccuracies, which caused delays in the nominations process. We made seven recommendations regarding nominations to the consolidated terrorist watchlist and the sharing of terrorism-related information. The components agreed with the recommendations and agreed to implement corrective actions.

- **The DEA's Controls over Weapons and Laptop Computers.** The OIG conducted a follow-up review examining whether the DEA has addressed weaknesses in its controls over its weapons and laptop computers identified in a 2002 OIG review. We determined that the DEA's rate of loss for weapons has increased since our 2002 review, while the rate of loss for laptops has declined. However, we found that the DEA could not determine what information was on its lost or stolen laptop computers, and the DEA was unable to provide assurance that lost or stolen laptop computers did not contain sensitive or personally identifiable information. We also found that many lost or stolen laptops were not protected by encryption software. In addition, DEA employees were not internally reporting lost or stolen weapons and laptops in a timely manner, and the DEA was not informing the Department of weapon and laptop losses or ensuring that relevant information about lost weapons and laptops was entered in the National Crime Information Center database. We made seven recommendations to improve the DEA's controls over weapons and laptops. The DEA agreed with six of the seven recommendations.

- **The Department's Victim Notification System.** This OIG review examined the Department's Victim Notification System (VNS), an automated system operated by the Executive Office for U.S. Attorneys (EOUSA) that notifies federal crime victims regarding developments in their cases. As part of the review, the OIG surveyed active and inactive crime victims about their use of the VNS. Survey respondents generally reported that they were satisfied with VNS services. However, some reported that they had not heard of the VNS prior to receiving the OIG survey, had never received a notification from the VNS, or were not even aware that they were registered as crime victims in the VNS. In addition, our audit found insufficient internal controls to ensure the accuracy and completeness of data in the VNS. We also identified deficiencies in the security of VNS information, most notably that sensitive crime

victim information contained within the VNS was not adequately protected. The OIG made 19 recommendations to help improve management of the VNS. EOUSA concurred with our recommendations and has outlined a plan to address them.

- **The FBI's Management of Confidential Case Funds and Telecommunication Costs.** This OIG audit examined the FBI's management of confidential case funds that support its undercover activities. The audit found that the FBI lacked an adequate financial system necessary to manage confidential case funds effectively. As a result, FBI employees developed various "work-arounds" to the system in an effort to track confidential case fund requests made by FBI special agents working in undercover capacities. However, the volume of undercover telephone bills, coupled with the inconsistent way various FBI field offices handled confidential case funds, resulted in the FBI routinely paying covert telecommunication costs late. These late payments sometimes resulted in telecommunication carriers terminating FBI surveillance delivery lines for non-payment. We also found that nearly half of the sampled employees who had daily access to confidential case funds had financial histories that indicated personal monetary problems. We recommended that the FBI improve its processing and tracking of confidential case funds, how it tracks and pays undercover telecommunication expenses, and its oversight of confidential case fund management. The FBI agreed with the recommendations and has begun to implement them.

- **The BOP's Efforts to Manage Inmate Health Care Costs.** This OIG review examined the $4.7 billion that the BOP spent on healthcare for inmates from fiscal years (FY) 2000 through 2007. The OIG found that the BOP has kept the growth of inmate health care costs over the past 7 years at a reasonable level compared to national health care cost data by implementing effective and efficient cost containment strategies. However, we found that BOP institutions did not always provide recommended preventive medical services to inmates and did not consistently provide inmates with the medical services recommended by BOP guidelines. In addition, the BOP allowed some health care providers to practice medicine without valid authorizations, and methods to accumulate and report health-related performance measures were inconsistent. We made 11 recommendations to help the BOP improve its provision of health care to inmates, and the BOP agreed with the recommendations.

Investigations

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

- An OIG investigation led to the arrest and suspension of an FBI security specialist who was responsible for negotiating, reviewing, and making recommendations for the purchase of more than $1.9 million in shredders. Investigators determined that the specialist accepted a paid family vacation valued at over $7,500 from the company that was awarded the shredder contract.

- An OIG investigation led to the arrest and resignation of an FBI financial manager who stole funds totaling $22,425 that were designated for undercover operations.

- An investigation led to the conviction of the former Mayor of Fairbanks, Alaska, on charges of theft of government funds, conspiracy, money laundering, and submitting false tax returns, and the guilty plea of his wife on charges of money laundering and theft of federal funds. The investigation developed evidence that the Mayor and his wife used federal grant funds that were designated to operate a non-profit organization to purchase a flat screen television and other items for their personal use and to partially fund the building of their church.

- A joint investigation determined that a BOP physician and physician's assistant and three civilians established a medical clinic and fraudulently billed Medicare approximately $2 million for HIV infusion therapy treatment that was not actually provided to patients. The BOP physician was sentenced to 2 years' incarceration while the BOP physician's assistant was sentenced to 20 months' incarceration. Two civilians were sentenced to 24 and 30 months' incarceration, respectively. The four defendants also were ordered to pay more than $1.8 million in restitution. Sentencing is pending for the third civilian.

- An investigation led to the arrest and guilty plea of a Department grantee who served as ombudsman for the Putnam County Sheriff's Department in Indiana and stole $57,916 in grant funds and $30,914 in general funds belonging to the Sheriff's Department. The grantee was sentenced to 18 months' incarceration and ordered to pay restitution to the Department and the Putnam County Sheriff's Department.

Ongoing Work

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

- The Department's removal of U.S. attorneys and alleged politicization in the hiring of Department career employees

- The FBI's use of exigent letters to obtain telephone records

- The FBI's involvement in and observations of detainee interrogations at Guantanamo Bay and in Iraq and Afghanistan

- The Department's involvement with the National Security Agency's Terrorist Surveillance Program

- The FBI's efforts to resolve terrorist threats and suspicious incidents

- Bureau of Alcohol, Tobacco, Firearms and Explosives' (ATF) controls over weapons, laptops, and other sensitive property

- The FBI's efforts to combat crimes against children

- The Department's major information technology (IT) vulnerabilities

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, ATF, USAO, U.S. Marshals Service (USMS), and all other organizations within the Department, as well as contractors of the Department and organizations receiving grant money from the Department.

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

- **Audit Division** is responsible for independent audits of Department programs, computer systems, and financial statements. The Audit Division has field offices in 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, Office of Operations, Office of Policy and Planning, and Advanced Audit Techniques Group.

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

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

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

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

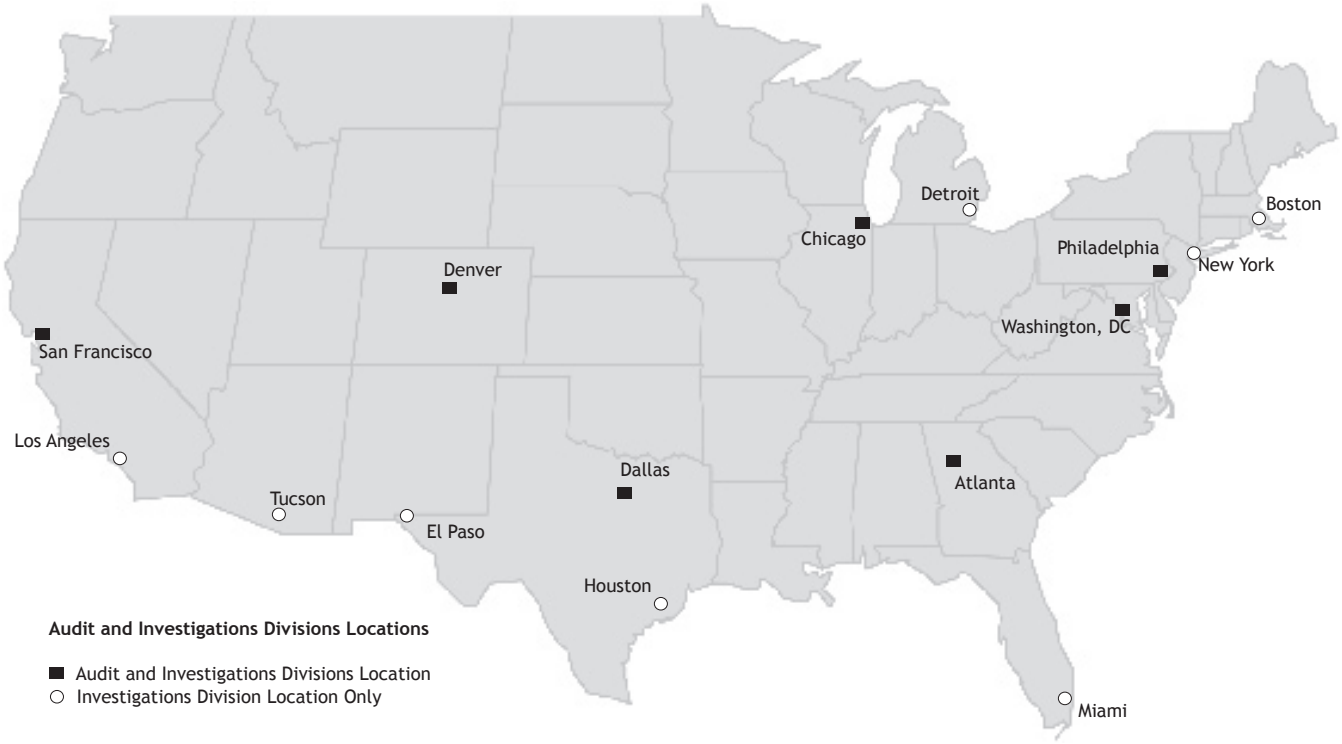
components in the areas of budget formulation and execution, security, personnel, training, travel, procurement, property management, information technology, computer network communications, telecommunications, quality assurance, internal controls, and general support.

- **Office of the 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 410 special agents, auditors, inspectors, attorneys, and support staff. For FY 2008, the OIG's direct appropriation was $71 million, and the OIG received an additional $3.5 million in reimbursements.

As required by Section 5 of the *Inspector General Act of 1978* (IG Act), as amended, this *Semiannual Report to Congress* reviewing the accomplishments of the OIG for the 6-month period of October 1, 2007, through March 31, 2008, is to be submitted no later than April 30, 2008, to the Attorney General for his review. The Attorney General is required to forward the report to Congress no later than May 31, 2008, along with information on the Department's position on audit resolution and follow-up activity in response to matters discussed in this report.

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



Multicomponent Audits, Reviews, and Investigations

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

Reports Issued

Audit of the Department's Terrorist Watchlist Nomination Processes

The OIG's Audit Division examined the Department's processes for nominating known or suspected terrorists to the consolidated terrorist watchlist. The FBI is the only Department component that formally nominates individuals to the consolidated terrorist watchlist. Between January 1, 2005, and November 29, 2007, the FBI processed over 8,000 watchlist nominations.

Our audit found that the FBI has developed a formal policy for nominating known or suspected terrorists to the watchlist, has sound record management procedures for its standard watchlist nominations, and has provided basic training on the watchlist nomination process to its staff. In addition, we found that the FBI has established criteria and quality controls to assist in developing proper and accurate watchlist nominations.

However, we found that FBI case agents did not always update watchlist records when new information became known, and the FBI did not always remove watchlist records when it was appropriate. Moreover, watchlist nomination submissions from FBI field offices often were incomplete or contained inaccuracies, which caused delays in the nominations process. Additionally, FBI field offices at times bypassed FBI headquarters and the FBI's internal controls by submitting nominations directly to the National Counterterrorism Center (NCTC). This practice may affect the completeness of FBI records that support the nominations forwarded for inclusion on the watchlist.

Although the FBI is the only component that officially nominates individuals for inclusion on the consolidated terrorist watchlist, other components – such as ATF, BOP, DEA, and USMS – have the potential to obtain terrorist-related information through their day-to-day operations and are required to share terrorism information with the FBI. However, at least one component (ATF) did not categorize criminal activity as being terrorism-related in a manner similar to the FBI, most notably in cases of domestic terrorism. As a result, the potential exists for terrorism information to not be shared with the FBI and for terrorists to not be watchlisted.

Another issue that arose during our audit related to the FBI, DEA, and U.S. National Central Bureau of Interpol (USNCB) preparing and

disseminating terrorist-related intelligence reports throughout the intelligence community. Although these agencies did not intend for their reports to be treated as official watchlist nominations, the NCTC used information from these intelligence reports to create watchlist records that were sourced to the FBI, DEA, and USNCB. However, because the agencies were not aware of this NCTC practice, they did not monitor these records to ensure that they were updated or removed when appropriate.

Finally, we found that although components are heavily involved in watchlisting and actively sharing terrorist information, these activities have been developed independently and are not coordinated by the Department. We recommended that the Department consider promulgating policy related to nominations to the consolidated terrorist watchlist and the sharing of information that might result in such a nomination. Such a standardized framework would allow other entities in the Intelligence Community, such as NCTC, to better understand the intent of, and act appropriately upon, the information received from Department components.

We made seven recommendations regarding nominations to the consolidated terrorist watchlist and the sharing of terrorism-related information. The components agreed with our findings and recommendations.

The Department's Key Indicators

The OIG's Audit Division examined the Department's key indicators that are used to measure annual progress toward achieving the four broad strategic goals contained in the Department's Strategic Plan for FYs 2003 – 2008. The Department's key indicators cover a broad range of measurements, including the number of terrorist acts committed by foreign nationals against U.S. interests within U.S. borders, the number of priority drug trafficking organizations disrupted and dismantled, the percent reduction in the DNA backlog, and the rate of assaults in federal prisons.

We concluded that components reporting on 12 of the 21 key indicators audited had adequate data collection and storage processes, sufficient data validation and verification processes, and complete and accurate disclosure of data limitations. However, we identified deficiencies and issues related to the remaining nine key indicators that could, and in some cases did, result in the inaccurate collection and reporting of data.

For example, we found that the FBI was not accurately reporting the number of child pornography websites or web hosts shut down as a result of its investigative efforts because it was counting the number of subpoenas it served on the web hosts rather than the number of actual sites that were shut down as a result of the subpoenas. We also found that the Department was not accurately reporting the percent of civil and criminal cases that were favorably resolved because USAOs and the litigating divisions were using different case disposition dates and at times were reporting the same cases, which resulted in double counting. In addition, the Department was not accurately measuring the reduction of homicides per site funded under its Weed and Seed Program because it was using data that included different grantees from year to year and thus were not comparable to draw a conclusion about yearly changes in the crime rate.

In response to our findings, the Department and affected components took action to modify its key indicator numbers for its FY 2007 Performance and Accountability report. We also made 12 recommendations to components and the Justice Management Division to help improve the data collection, storage, validation,

and verification processes and data limitation disclosures for the Department's key indicators. The Department and the components agreed with our recommendations.

Civil Rights and Civil Liberties Complaints

Section 1001 of the *USA Patriot Act* directs the OIG to receive and review complaints of civil rights and civil liberties abuses by Department employees, to publicize how people can contact the OIG to file a complaint, and to submit a semiannual report to Congress discussing our implementation of these responsibilities. In February 2008, the OIG issued its 12th report summarizing its Section 1001 activities during the period from July 1, 2007, to December 31, 2007.

The OIG's most recent report described the number of complaints we received under this section, the cases that were opened for investigation, and the status of these cases. In addition, the report described the status of the OIG's follow-up reviews of the FBI's use of national security letters and Section 215 orders for business records in 2006.

The report described other OIG reviews that examined civil rights and civil liberties-related issues, including an audit of the Terrorist Screening Center; an audit of the Department's Watchlist Nomination Process; and a review of FBI employees' observations and actions regarding alleged abuse of detainees at Guantanamo Bay and in Iraq and Afghanistan.

The Department's Financial Statement Audits

The *Chief Financial Officers Act of 1990* and the *Government Management Reform Act of 1994* require annual financial statement audits of the Department. The OIG's Audit Division oversees and issues the reports based on the work performed by independent public accountants. During this reporting period, we issued the report for the Department's Annual Financial Statement for FY 2007.

The Department received an unqualified opinion on its FY 2007 and 2006 financial statements. For FY 2007, the Department had two significant deficiencies at the consolidated level, compared to one material weakness and one reportable condition for FY 2006. Effective for FY 2007, the term "reportable condition" was changed to the term "significant deficiency," and new definitions of material weakness and significant deficiency were introduced in U.S. government auditing standards.

Both of the Department's significant deficiencies are repeat issues, which were reported as one material weakness and one reportable condition in FY 2006. For FY 2007, weaknesses in the general and application controls for each of the Department's component financial systems were reported as a significant deficiency, with the exception of the FBI where it was classified as a material weakness.

The Department's significant deficiency related to financial reporting and includes several serious but isolated issues, including the USMS's financial accounting and reporting quality-control and assurance and funds management controls; ATF's accounts payable process; Office of Justice Programs' (OJP) grant advance and payable estimation process and grant deobligation process; Offices, Boards and Divisions' status of obligations controls and preparation, review, and approval of journal entries; and Assets Forfeiture Fund and Seized Asset Deposit Fund's obligations and disbursements controls and seized and forfeited property controls.

While the Department's financial statement audit results have continued to improve, the Department still lacks sufficient automated systems to readily support ongoing accounting operations and financial statement preparation. Inadequate, outdated, and in some cases non-integrated financial management systems do not provide certain automated financial transaction processing activities that are necessary to support management's need for timely and accurate financial information throughout the year. Many tasks still must be performed manually at interim periods and at year's end, requiring extensive manual 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. While the Department is moving towards implementing a Unified Financial Management System that it believes will correct many of these issues, implementation has been slow and will not be completed across the Department for at least another 5 years.

The FY 2007 consolidated report on compliance and other matters identified no instances of significant non-compliance with applicable laws and regulations. Although some instances of non-compliance were reported at some of the components, the consolidated report determined that none of the component level non-compliance issues caused the Department as a whole to be in significant non-compliance.

Comparison of FY 2007 and 2006 Audit Results

Reporting Entity	Auditors' Opinion on Financial Statements		Number of Material Weaknesses[1]				Number of Significant Deficiencies[2]			
			Financial		Information Systems		Financial		Information Systems	
	2007	2006	2007	2006	2007	2006	2007	2006	2007	2006
Consolidated Department of Justice	U[3]	U	0	0	0	1	1	1	1	0
Offices, Boards and Divisions	U	U	0	0	0	0	2	0	1	1
Assets Forfeiture Fund and Seized Asset Deposit Fund	U	U	0	0	0	0	2	1	1	1
Federal Bureau of Investigation	U	U	0	0	1	1	0	0	0	0
Drug Enforcement Administration	U	U	0	0	0	0	0	0	1	0
Office of Justice Programs	U	U	0	1	0	1	2	1	1	0
U.S. Marshals Service	U	U	2	1	0	1	0	0	1	0
Federal Bureau of Prisons	U	U	0	0	0	0	0	0	1	1
Federal Prison Industries, Inc.	U	U	0	0	0	0	0	0	1	0
Working Capital Fund[4]	N/A	U	N/A	0	N/A	0	N/A	1	N/A	1
Bureau of Alcohol, Tobacco, Firearms and Explosives	U	U	1	1	0	1	0	0	1	0
Component Totals			***3***	***3***	***1***	***4***	***6***	***3***	***8***	***4***

[1] A material weakness is a significant deficiency (see below) or combination of significant deficiencies that result in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the Department's internal control.

[2] A significant deficiency is a control deficiency or combination of control deficiencies that adversely affects the Department's ability to initiate, authorize, record, process, or report financial data reliably in accordance with U.S. generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the Department's consolidated financial statements that is more than inconsequential will not be prevented or detected by the Department's internal control over financial reporting. A control deficiency exists when the design or operation of a control does not allow management or employees in the normal course of performing their assigned functions to prevent or detect and correct misstatements on a timely basis.

[3] An unqualified opinion is 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.

[4] Beginning in FY 2007, the activities and balances of the Working Capital Fund, previously reported separately, have been included in the financial statements of the Offices, Boards and Divisions.

Investigations

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

- A multi-agency investigation that included the OIG's Fraud Detection Office led to the arrest of two civilian brothers on charges of conspiracy and trafficking of counterfeit goods. The indictment returned in the Southern District of Texas alleged that the brothers intentionally trafficked counterfeit computer networking cards into the United States. The computer cards were shipped from China and used by customers that included the FBI, BOP, U.S. Marine Corps, U.S. Air Force, Federal Aviation Administration, Department of Energy, and multiple defense contractors, universities, school districts, and financial institutions. Judicial proceedings continue.

Ongoing Work

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

The OIG and the Department's Office of Professional Responsibility are conducting a joint review of the Department's removal of several U.S. attorneys. The joint review also is investigating allegations that Department personnel used political considerations in assessing candidates for career Department positions. In addition, the joint review is examining whether Department employees improperly considered applicants' political affiliations when hiring for the Department's entry-level Honors Program and Summer Law Intern Program from 2002 through 2006.

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

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

Assessment of Major IT Vulnerabilities

The Department's operations have become increasingly dependent on IT systems and the information contained within those systems. This OIG audit is identifying the Department's major IT vulnerabilities and assessing actions taken to mitigate them. The audit also is determining the extent to which the Department has communicated the Office of Management and Budget's IT security requirements to its components.

Sex Offender Registration

The OIG is reviewing the Department's efforts to implement the *Sex Offender Registration and Notification Act* (Title I of the *Adam Walsh Child Safety and Protection Act* of 2006). We are reviewing how the Department is identifying, investigating, arresting, and prosecuting fugitive sex offenders who failed to register or update their registrations. We also are determining the status

of the Department's efforts to create and maintain national sex offender registries and provide guidance and assistance to states regarding the maintenance of their sex offender registries.

Prison Staff Sexual Abuse of Inmates

The OIG is reviewing the Department's efforts to prevent sexual abuse of federal inmates and detainees by BOP and USMS staff. Our review is examining whether the Department is implementing adequate policies and procedures for addressing sexual abuse issues, investigating allegations of abuse, and prosecuting substantiated cases.

Review of Legislative and Public Affairs Expenses

In response to a directive in the 2008 *Consolidated Appropriations Act*, the OIG is conducting an audit of legislative and public affairs expenses within the Department, including expenses of the legislative and public affairs offices of Department components.

Federal Bureau of Investigation

The FBI is responsible for counterterrorism, foreign counterintelligence, and for addressing other national security threats. The FBI also investigates cyber crimes, public corruption, civil rights violations, organized crime, violent crimes, and other violations of federal law. FBI Headquarters in Washington, D.C., coordinates the activities of more than 30,000 employees in 56 domestic field offices, approximately 400 satellite offices, and 61 foreign liaison posts overseas that are responsible for the wide range of national security, criminal, and other matters within the FBI's jurisdiction.

Reports Issued

The FBI's Use of National Security Letters in 2006

In March 2008, the OIG issued its second report evaluating the FBI's use of national security letters (NSL). Under five statutory provisions, the FBI can use NSLs to obtain records, such as toll billing records and subscriber information from telephone companies, transactional records from Internet service providers, bank records from financial institutions, and full or limited consumer credit information from credit reporting agencies.

The *USA Patriot Improvement and Reauthorization Act of 2005* (Patriot Reauthorization Act) directed the OIG to conduct two reviews of the FBI's use of NSLs. Our first report, issued in March 2007, reviewed the FBI's use of NSLs from 2003 through 2005. We found serious and widespread misuse of NSL authorities, such as issuing NSLs without proper authorization, making improper requests under the statutes cited in the NSLs, and conducting unauthorized collection of telephone or Internet e-mail transactional records.

In our follow-up report issued in March 2008, we determined that the FBI and the Department have made significant progress implementing recommendations in our first report and adopting corrective actions to address the serious problems we identified. Measures implemented by the FBI include a new NSL data system designed to facilitate the issuance and tracking of NSLs and ensure accurate reports to Congress and the public on NSL usage; issuing NSL guidance memoranda and conducting training of field and headquarters personnel; and creating a new Office of Integrity and Compliance modeled after private sector compliance programs. We also found that the FBI has devoted substantial time, energy, and resources ensuring that its field managers and agents understood the seriousness of the FBI's shortcomings in its use of NSLs and their responsibility for correcting these deficiencies.

In addition, the Department's National Security Division instituted periodic national security reviews of FBI field and Headquarters divisions to assess whether the FBI was using various intelligence techniques, including NSLs, in

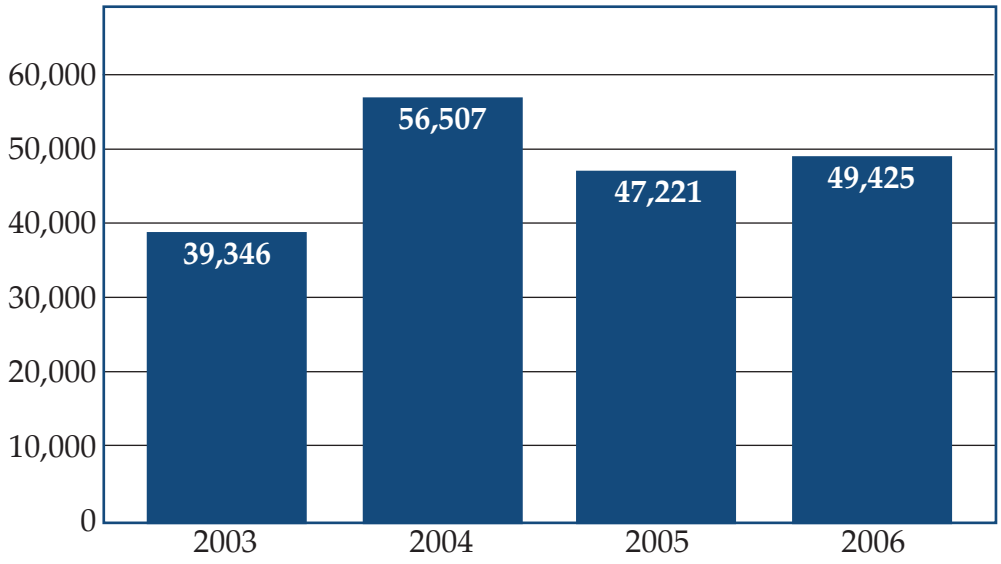
accordance with applicable laws, guidelines, and policies.

Our report also analyzed three NSL reviews conducted by the FBI following the release of our first report. One review examined a random 10 percent sample of counterterrorism, counterintelligence, and foreign computer intrusion cyber investigation case files active in FBI field offices between 2003 and 2006. This review confirmed the types of NSL-related deficiencies and possible intelligence violations that we identified in our first report. The FBI's statistically valid sample of field case files found a rate of NSL violations (9.43 percent) higher than what we found (7.5 percent) in the non-statistical sample of NSLs we examined in our first report.

Regarding NSL usage in 2006, we found a continued upward trend in the use of NSLs, with 49,425 NSL requests issued in 2006 – a 4.7 percent increase from the previous year. For the 4-year period, from 2003 through 2006, the FBI issued more than 192,000 NSL requests. On average, approximately one-third of all counterterrorism, counterintelligence, and cyber investigations that were open at any time during 2006 employed NSLs. Our review also found that the percentage of NSL requests related to investigations of U.S. persons continued to increase, from approximately 39 percent of all NSL requests in 2003 to approximately 60 percent in 2006.

In response to the directive in the Patriot Reauthorization Act to identify any "improper or illegal" use of NSLs, we described 84 possible intelligence violations involving the use of NSLs in 2006 that were self-reported to FBI Headquarters. Of these 84 possible violations, the FBI concluded that 34 needed to be reported to the President's Intelligence Oversight Board (IOB) in 2006. The 34 matters that were reported included errors, such as issuing NSLs without proper authorization, improper requests, and unauthorized collection of telephone or Internet e-mail records. We found that 20 of these violations were attributable to mistakes made by the FBI, while 14 resulted initially from mistakes by recipients of NSLs. The number of possible intelligence violations identified by FBI personnel in 2006 was significantly higher than

NSL Requests (2003 through 2006)



the 26 violations reported from 2003 through 2005, of which 19 were reported to the IOB. We believe that the increase may be due in large part to the attention garnered by our first NSL review and to increased training, guidance, and oversight by the FBI. Although the number of self-reported violations increased, the large number of unreported violations found during the FBI's three NSL reviews demonstrated that the overwhelming majority of violations were not identified and self-reported by the FBI.

As directed by the Patriot Reauthorization Act, we also examined whether NSLs issued after the effective date of the Patriot Reauthorization Act contained the required certifications to impose non-disclosure and confidentially requirements on NSL recipients. In the random sample of NSLs we reviewed, we found that 97 percent of the NSLs imposed non-disclosure and confidentiality requirements and almost all contained the required certifications. We found that a small percentage of the justifications for imposing this requirement were perfunctory and conclusory, and a small number of the NSL approval memoranda failed to comply with internal FBI policy.

We made 17 additional recommendations to help improve the FBI's use and oversight of NSLs, including to provide additional guidance and training for FBI agents on the proper use of NSLs and on the reviewing, filing, and retention of NSL-derived information; reinforce the need for FBI agents and supervisors to determine whether there is adequate justification for imposing non-disclosure and confidentiality requirements on NSL recipients; regularly monitor the preparation and handling of NSLs; and provide timely reports of possible intelligence violations to FBI Headquarters. The FBI agreed with the recommendations and said it would implement additional actions to address our findings.

The FBI's Use of Section 215 Orders for Business Records in 2006

In March 2008, the OIG issued a follow-up report on the FBI's use of Section 215 orders to obtain business records. Section 215 of the *USA Patriot Act* allows the FBI to seek an order from the Foreign Intelligence Surveillance Act (FISA) Court to obtain "any tangible thing," including books, records, and other items, from any business, organization, or entity provided that the item or items are for an authorized investigation to protect against international terrorism or clandestine intelligence activities.

Our first report, issued in March 2007, examined the FBI's use of this authority from 2002 through 2005. The Department's Office of Intelligence Policy and Review, on behalf of the FBI, submits two different types of Section 215 applications to the FISA Court: "pure" Section 215 applications and "combination" Section 215 applications. A "pure" Section 215 application refers to a Section 215 application for any tangible item, and it is not associated with any other FISA authority. A "combination" Section 215 application refers to a Section 215 request that is added to a FISA application for pen register/trap and trace orders, which identify incoming and outgoing telephone numbers called on a particular line. We also found two instances involving improper use of Section 215 orders in 2005 and significant delays within the FBI and the Department in processing requests for Section 215 orders throughout the time period that we reviewed.

Our second report examined the FBI's use of Section 215 orders in 2006 and, as required by the Patriot Reauthorization Act, the minimization procedures for business records that the Attorney General was required to adopt in 2006. We found that the FBI and the Department processed 15 "pure" Section 215 applications and

32 "combination" Section 215 applications in 2006 that were formally submitted to and approved by the FISA Court. Six additional 215 applications were withdrawn by the FBI before they were formally submitted to the FISA Court. Our review found that FBI agents encountered similar processing delays for Section 215 applications as those identified in our previous report. However, both the FBI and Office of Intelligence Policy and Review were able to expedite two Section 215 requests in 2006 when the FBI identified them as emergency requests.

Our review did not identify any illegal use of Section 215 orders in 2006. However, we found two instances when the FBI received more information than it requested in the Section 215 orders. In one case, approximately 2 months passed before the FBI recognized it was receiving additional information that was beyond the scope of the FISA Court order. The FBI reported this incident to the IOB, and the additional information was sequestered with the FISA Court. In the other case, the FBI quickly determined that it inadvertently received information not authorized by the Section 215 order and isolated the records. However, the FBI subsequently concluded that the matter was not reportable to the IOB and that it should be able to use the material as if it were "voluntarily produced" because the information was not statutorily protected. We disagreed with this conclusion, and our report recommended that the FBI develop procedures for identifying and handling information that is produced in response to, but outside the scope of, the Section 215 order.

In response to the Patriot Reauthorization Act's directive to identify any "noteworthy facts or circumstances" related to the use of Section 215 orders, our report discussed another case in which the FISA Court twice refused to authorize a Section 215 order based on concerns that the investigation was premised on protected First Amendment activity. The FBI subsequently issued NSLs to obtain information based on the same factual predicate and without a review to ensure the investigation did not violate the subject's First Amendment rights. We questioned the appropriateness of the FBI's actions because the NSL statute contains the same First Amendment caveat as the Section 215 statute.

Finally, as directed by the Patriot Reauthorization Act, we examined the interim procedures adopted by the Department for Section 215 orders to minimize the retention and prohibit the dissemination of non-publicly available information about U.S. persons. We concluded that the interim minimization procedures adopted in September 2006 do not provide specific guidance for minimization procedures that the Patriot Reauthorization Act appeared to contemplate. The OIG report recommended that the Department develop specific minimization procedures related to Section 215 orders.

We provided the full classified report to Congress, the Department, the FBI, and the Office of the Director of National Intelligence.

The FBI's Management of Confidential Case Funds and Telecommunication Costs

The OIG's Audit Division examined the FBI's management of confidential case funds that support its undercover activities. The FBI uses confidential funds to conceal its identity from criminals, vendors, or the public during an undercover activity or operation. The audit stemmed from a recently concluded OIG investigation in which an FBI telecommunications specialist in a field office pled guilty to stealing over $25,000 in confidential funds intended for undercover telecommunication services. The

investigation also revealed that the employee took advantage of weak controls over field division confidential funds to convert FBI money for her own use.

The audit found that the FBI lacked an adequate financial system to manage confidential case funds effectively. FBI field divisions used an antiquated information system called the Financial Management System to process confidential case fund expenditures. The Financial Management System could not track details pertaining to confidential payments, such as commercial vendor names, invoice numbers, or whether a supported case was open or closed. Consequently, FBI employees were left to develop various "work-arounds" to the system in an effort to track confidential case fund requests made by FBI special agents working in undercover capacities. As a result of the audit, the FBI agreed to revise its plans for a new financial management information system to replace its antiquated system.

Since the FBI treats telephone surveillance bills as confidential case costs, the audit examined the procedures used by FBI field divisions to pay these bills. The audit discovered that the volume of undercover telephone bills, coupled with the inconsistent way various FBI field offices handled confidential case funds, resulted in the FBI routinely paying covert telecommunication costs late. These late payments sometimes resulted in telecommunication carriers terminating FBI surveillance delivery lines for non-payment.

In examining the personnel and security files of FBI field division employees who had daily access to confidential case funds, we found that nearly one-half of the sampled employees had financial histories that indicated personal monetary problems, such as late loan payments and bankruptcies. Our audit noted that the FBI had not developed procedures specifically to ensure that employees with financial concerns were not placed in situations where they could process confidential case funds without enhanced supervision.

The audit recommended that the FBI improve its processing and tracking of confidential case funds, how it tracks and pays undercover telecommunication expenses, and its oversight of confidential case fund management. The FBI agreed with the recommendations and has begun to implement them.

Implementation of the *Communications Assistance for Law Enforcement Act*

In 1994, Congress passed the *Communications Assistance for Law Enforcement Act* (CALEA) to enable court-ordered electronic surveillance in light of the rapid deployment of new technologies and wireless communication services. To facilitate CALEA implementation, Congress appropriated nearly $500 million to the Telecommunications Carrier Compliance Fund (TCCF). The Attorney General designated the FBI to manage the TCCF and reimburse telecommunications carriers for the cost of modifying equipment, facilities, or services installed or deployed before 1995.

Under CALEA, the OIG biennially reports to Congress on the equipment, facilities, and services modified to comply with CALEA requirements. Our sixth CALEA audit, issued in March 2008, found that over a 10-year period the FBI spent nearly $452 million on licensing agreements with manufacturers to provide CALEA solutions on equipment used by telecommunications carriers. In addition to these licensing agreements, the FBI directed nearly $7.5 million in TCCF funds to pay wire line carriers for deploying, activating, and testing CALEA solutions. By the end of 2007,

the FBI had expended a total of $459 million in TCCF funds, and Congress rescinded over $40 million from the TCCF. Our audit found that only $5,037 remained in the TCCF, and that the FBI is working with the Department to transfer the remaining funds to the Working Capital Fund.

We also found that the FBI has continued to develop tools and implement resources to help facilitate and measure CALEA compliance of various telecommunications providers. The FBI hosted and attended forums and other types of meetings with law enforcement personnel, developed and updated its "AskCALEA" website, conducted and issued annual threat assessment surveys, and surveyed telecommunications providers regarding the status of CALEA solutions on their networks. In light of the TCCF rescissions, the FBI is concentrating its efforts on working with and testing new telecommunications providers to ensure that CALEA solutions are developed and deployed for emerging technologies.

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 audited several state and local laboratories that participate in CODIS to determine if they comply with the FBI's Quality Assurance Standards and National DNA Index System (NDIS) requirements. Additionally, we evaluated whether the laboratories' DNA profiles in CODIS databases were complete, accurate, and allowable. Below are examples of our audit findings:

- The Tulsa Police Department Forensic Laboratory in Tulsa, Oklahoma, was in compliance with the standards governing CODIS activities with the following exceptions. First, the Tulsa Laboratory was storing weekly backup server tapes in a manner inconsistent with NDIS security requirements. Second, the Laboratory uploaded two forensic profiles into NDIS without making it clear which sample was from the suspect and which sample was obtained from the victim's husband in order to eliminate him as a source of the DNA. The Laboratory agreed with and addressed all of our findings before audit work was completed. Therefore, we made no formal recommendations.

- The Utah Department of Public Safety Bureau of Forensic Services Laboratory in Salt Lake City, Utah, was in compliance with the standards governing CODIS activities with the following exceptions. We noted exceptions with the Laboratory's compliance with security requirements regarding CODIS user accounts, concurrent login restriction controls, and the frequency of changing passwords. We also found that the Laboratory stored evidence in an unsecured short-term container – a practice that did not fully comply with quality assurance standards. Finally, the Laboratory did not submit its external quality assurance audit to the FBI within the required 30 days due to a miscommunication. Laboratory officials have since taken corrective action to address these deficiencies. We made two recommendations, and the FBI agreed with both recommendations.

Investigations

During this reporting period, the OIG received 928 complaints involving the FBI. The most common allegations made against FBI employees were IOB violations, job performance failure,

waste, misuse of government property, and off-duty misconduct. The OIG opened 18 cases and referred other allegations to the FBI's Inspection Division for its review.

At the close of the reporting period, the OIG had 44 open criminal or administrative investigations of alleged misconduct related to FBI employees. The criminal investigations covered a wide range of offenses, including release of information, waste, and job performance failure. The administrative investigations involved serious allegations of misconduct. The following are examples of cases involving the FBI that the OIG's Investigations Division handled during this reporting period:

- An investigation by the OIG's Washington Field Office led to the arrest of an FBI security specialist on charges of accepting an illegal gratuity. OIG investigators determined that the security specialist, who was responsible for negotiating, reviewing, and making recommendations for the purchase of more than $1.9 million of office shredders, accepted a paid family vacation valued at over $7,500 from the company that was awarded the shredder contract. The security specialist is on indefinite suspension from the FBI. Judicial proceedings continue.

- An investigation by the OIG's Chicago Field Office led to the arrest of an FBI financial manager on charges of embezzlement of government funds. The investigation determined that the financial manager stole funds totaling $22,425 that were designated for undercover operations for her own personal use. She also falsified receipts to make it appear that invoices were paid, but instead deposited the money into her own bank accounts. The financial manager resigned her position as a result of our investigation. Judicial proceedings continue.

- An investigation by the OIG's Washington Field Office determined that an FBI special agent, without authorization, arranged for the use of an FBI undercover real estate company to conduct a private real estate transaction – the sale of a $1.3 million home – that benefited her personal friends. The investigation also disclosed that the special agent facilitated the FBI's lease of an apartment for undercover purposes on property where she had a personal interest and then used the apartment for unauthorized personal purposes. Although the special agent obtained approval from management before entering into the undercover rental agreement, she did not disclose to the FBI her personal ties to the property. Based on the OIG's investigation, the FBI notified the special agent that it was proposing her dismissal for her lack of candor during the OIG investigation.

- The OIG's Dallas Field Office investigated allegations that an FBI supervisory language specialist assigned to the Language Support Program encouraged subordinates to report fraudulent time and attendance invoice statements of their work and accepted gifts from subordinates. The investigation determined that during the supervisory language specialist's tenure there was no system to properly account for linguists' daily hours, billing records submitted by linguists did not always match the times worked, and linguists were permitted to work off-site without proper approval. The investigation also concluded that the supervisory language specialist accepted gifts from subordinates and, in violation of contract terms and without FBI oversight, provided pre-signed blank authorization request forms for overtime/holiday pay to linguists. The FBI terminated the supervisory language specialist from her position based on her dereliction of

supervisory responsibilities and her lack of candor during her OIG interview.

Ongoing Work

The FBI's Use of Exigent Letters and Other Improper Requests

As a follow-up to our reviews of the FBI's use of NSLs, the OIG is investigating the FBI's use of exigent letters and other improper requests to obtain telephone records. We previously reported on a practice by which the FBI used over 700 exigent letters rather than NSLs to obtain telephone toll billing records. We determined that by issuing exigent letters rather than NSLs the FBI circumvented the NSL statutes and violated the Attorney General's Guidelines and internal FBI policy. Our forthcoming report is examining in greater detail the FBI's use of exigent letters and its issuance of "blanket" NSLs used to "cover" or "validate" the information obtained from exigent letters and other improper requests.

FBI Reports of Alleged Abuse of Military Detainees

The OIG is reviewing FBI employees' observations and actions regarding alleged abuse of detainees at Guantanamo Bay, Abu Ghraib prison, and other venues controlled by the U.S. military. The OIG is examining whether FBI employees participated in any incident of detainee abuse, whether FBI employees witnessed incidents of abuse, whether FBI employees reported any abuse, and how those reports were handled by the FBI. In October 2007, a draft report was provided to the Department, FBI, Department of Defense, and Central Intelligence Agency for comment and classification review. That review is ongoing.

The FBI's Efforts to Combat Crimes Against Children

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

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

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

The FBI's Watchlist Nomination Practices

As a follow-up to our audit of the Department's watchlist nomination processes, we are examining

in more detail the FBI's practices for nominating individuals to the consolidated terrorist watchlist. This review includes determining if the FBI appropriately places individuals on the watchlist in a timely manner, if records are updated with new information, and if individuals are removed from the watchlist in a timely manner.

Sentinel IV: Status of the FBI's Case Management System

The OIG is assessing the status of the Sentinel project. We are evaluating whether the FBI's management controls and provisions of the Sentinel contract provide reasonable assurance that Sentinel will be completed on time and within budget.

Review of the FBI's Disciplinary System

The OIG is reviewing the FBI's system for reporting and investigating allegations of employee misconduct and for disciplining employees who are found to have committed misconduct. This is the fifth in a series of reviews of Department component disciplinary systems.

The FBI's Foreign Language Translation Services

This review is assessing the FBI's progress in translating foreign language material. As a follow-up to our July 2004 audit, the OIG is assessing the extent of any translation backlogs and the efforts taken by the FBI to address them. We also are determining if controls are in place to ensure appropriate prioritization of work, accurate and timely translations, and proper security of sensitive information.

The FBI's Security Check Procedures for Immigration Applicants

The OIG is examining the FBI's name check and fingerprint identification checks for immigration applications.

Federal Bureau of Prisons

The BOP operates a nationwide system of prisons and detention facilities to incarcerate individuals imprisoned for federal crimes and detain those awaiting trial or sentencing in federal court. The BOP has approximately 36,000 employees and operates 114 institutions, 6 regional offices, and 2 staff training centers. The BOP is responsible for the custody and care of approximately 201,000 federal offenders, 166,100 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.

Reports Issued

The BOP's Efforts to Manage Inmate Health Care Costs

The BOP is responsible for delivering health care to federal inmates in its 114 institutions. From FYs 2000 through 2007, the BOP spent about $4.7 billion for inmate health care. In our review of the growth of inmate health care costs over the past 7 years, we found that the BOP has kept this growth at a reasonable level compared to national health care cost data reported by the Departments of Health and Human Services and Labor. The BOP has implemented cost containment strategies over the past several years to provide health care in a more effective and efficient manner. However, it generally does not maintain analytical data to assess the impact that individual initiatives have had on health care costs.

Our review also found that, with respect to inmate health care, BOP institutions did not always provide recommended preventive medical services to inmates. In addition, our audit determined that BOP institutions did not consistently provide inmates with the medical services recommended by BOP guidelines, which could lead to exacerbation of inmate medical conditions, higher costs for health care, medical-related complaints and lawsuits from inmates, and BOP liability for lack of adequate medical care.

In addition, we found that the BOP allowed some health care providers to practice medicine without valid authorizations, which increases the risk that they may provide medical services without having the qualifications, knowledge, skills, and experience necessary to correctly perform the services. We also calculated that 48 percent of BOP health care providers did not have their practices peer-reviewed to ensure the quality of their medical care, as required by BOP policy.

Prior OIG audits of BOP medical contracts identified contract-administration deficiencies in the BOP's review of health care costs, such as inadequate review and verification of contractor invoices and inadequate supporting documentation for billings. Subsequent to these audits, the BOP took action to address individual deficiencies at the institutions audited. However, our current

audit found that other BOP institutions still lacked appropriate controls in these areas, which indicates the existence of systemic weaknesses that are not being addressed by the BOP.

The BOP monitors its health care providers by performing program reviews of institution operations, reviewing medical provider skills and qualifications, and providing authorization documents based on the review results. Institutions also are required to accumulate and submit data on health-related performance measures to BOP headquarters. We determined that the BOP's methods to accumulate and report health-related performance measures were inconsistent, and that the data was not analyzed to evaluate the performance of BOP institutions. While the BOP has corrected deficiencies at the specific institutions where its program reviews found weaknesses, it did not develop and issue guidance to correct systemic deficiencies found during the reviews.

The OIG made 11 recommendations regarding the provision of inmate health care, and the BOP agreed with all of the recommendations.

Investigations

During this reporting period, the OIG received 2,680 complaints involving the BOP. The most common allegations made against BOP employees included official misconduct and force, abuse, and rights violations. The vast majority of complaints dealt with non-criminal issues that the OIG referred to the BOP's Office of Internal Affairs for review.

At the close of the reporting period, the OIG had 249 open cases of alleged misconduct against BOP employees. The criminal investigations covered a wide range of allegations, including bribery, introduction of contraband, and sexual abuse. The following are examples of cases involving the BOP that the OIG's Investigations Division handled during this reporting period:

- In our September 2007 *Semiannual Report to Congress*, we reported on an investigation conducted by the OIG's New York Field Office that led to the arrest of 11 BOP correctional officers charged with violating the civil rights of inmates at the Metropolitan Detention Center in Brooklyn, New York. In the first incident in November 2002, five correctional officers participated in a planned beating of an inmate and then attempted to disguise the attack by planting a noose in the inmate's cell and claiming in written reports that the inmate became combative as they attempted to prevent him from committing suicide. A second incident occurred in April 2006 where five correctional officers, including one who participated in the previously described attack, physically assaulted a different inmate in an elevator while escorting him to a special housing unit within the facility. These five correctional officers and two additional officers were charged with writing false reports concerning this incident.

  During this reporting period, a BOP captain, BOP lieutenant, and three additional correctional officers were convicted in the Eastern District of New York on charges of conspiracy to violate the civil rights of an inmate, obstruction of justice, and making false statements. Five additional correctional officers pled guilty to similar charges and one correctional officer was acquitted. The BOP lieutenant was sentenced to 2 years' incarceration followed by 3 years' supervised release. One of the correctional officers was sentenced to 4 months' incarceration followed by 6 months' home confinement and 3 years'

supervised release. Sentencing is pending for the other eight defendants.

- An investigation by the OIG's Dallas Field Office led to the arrest and guilty plea of a BOP chaplain for sexual abuse of a ward. Our investigation determined that on multiple occasions the chaplain, a Catholic priest, engaged in sexual acts with inmates who attended his Bible study class or who served as a clerk for the Religious Services Department at the prison. During an OIG interview, the chaplain admitted to multiple sexual acts with multiple victims and subsequently resigned his position with the BOP. Sentencing is pending.

- An investigation by the OIG's Atlanta Area Office led to the arrest and guilty plea of a BOP correctional officer on charges of bribery. OIG investigators determined that the correctional officer introduced marijuana and tobacco products into the prison for numerous inmates in exchange for money. Western Union records revealed that the correctional officer received at least 26 wire transfer payments from inmate family members or associates totaling more than $22,000. In an OIG interview, the correctional officer admitted to receiving $20,000 to $30,000 over an 18-month period for introducing contraband into the prison. The correctional officer resigned his position immediately following the interview. He was sentenced in the Northern District of Georgia to 1 year incarceration followed by 3 years' supervised released, and he was ordered to perform 120 hours of community service.

- An investigation by the OIG's Atlanta Area Office led to the arrest and guilty plea of a BOP correctional officer on charges of bribery and smuggling contraband into a federal prison. OIG investigators developed evidence that on several occasions the correctional officer provided inmates with cigarettes in exchange for money. The correctional officer was sentenced to 25 months' incarceration followed by 2 years' supervised release and was ordered to pay a $1,500 fine. The correctional officer resigned his position with the BOP as a result of our investigation.

- A joint investigation by the OIG's Denver Field Office and the Department of Homeland Security (DHS) Bureau of Immigration and Customs Enforcement led to the arrest of a BOP warehouse supervisor on federal charges of transportation of child pornography. The investigation determined that the warehouse supervisor possessed and transmitted child pornography through his personal computer to servers located in France. Judicial proceedings continue.

- A joint investigation by the OIG's Miami Field Office, FBI, Florida Department of Law Enforcement, and Department of Health and Human Services OIG led to the arrest and guilty plea of a BOP physician and physician's assistant and three civilians on charges of conspiracy to commit healthcare fraud. The investigation uncovered a scheme in which the five defendants established a medical clinic that was used to defraud the Medicare program by billing Medicare for HIV infusion therapy treatment that it was not providing. The clinic received approximately $2 million in fraudulent Medicare proceeds. The BOP physician was sentenced to 2 years' incarceration followed by 3 years' supervised release, fined $10,000, and ordered to perform community service. The BOP physician's assistant was sentenced to 20 months' incarceration followed by 24 months' supervised release. Two of the civilians were sentenced to 24 and 30 months' incarceration, respectively, followed by 24 months' supervised release. The four defendants also were ordered to pay more

than $1.8 million in restitution. Sentencing is pending for the third civilian. The physician and physician's assistant resigned from the BOP as a result of our investigation.

- A joint investigation by the OIG's Fraud Detection Office, Defense Criminal Investigative Service, U.S. Army Criminal Investigation Division, and U.S. Air Force Office of Special Investigations led to an agreement by Sioux Manufacturing Corporation (SMC) of Ft. Totten, North Dakota, to pay $2 million to settle allegations that it knowingly provided substandard woven Kevlar cloth for use in military combat helmets. Investigators determined that from approximately 1994 to 2006 SMC sold finished armored cloth (Kevlar) to Federal Prison Industries, Inc. (UNICOR), which used the Kevlar to manufacture Personnel Armor System Ground Troops helmets and sold the helmets to the Defense Logistics Agency. With each delivery of the Kevlar, SMC certified to UNICOR that its product met the required military specifications, one of which dictates a specific number of woven yarns per square inch of finished cloth.

  However, investigators found evidence that SMC sometimes delivered cloth that had not been woven to the required specifications. The helmets containing cloth woven by SMC passed all ballistics safety tests conducted pursuant to government contracts and similar tests conducted by the military during this investigation. Two former SMC employees filed the original lawsuit against the corporation under the qui tam or whistleblower provisions of the *False Claims Act*. The settlement was coordinated by the USAO for the District of North Dakota with the assistance of the Civil Division's Commercial Litigation Branch.

- In our September 2006 *Semiannual Report to Congress*, we reported on a joint investigation by the OIG's Houston Area Office and the DHS OIG that led to the arrest of a senior BOP correctional officer on charges of theft of public funds and wire fraud. The investigation disclosed that the correctional officer falsely claimed to be a victim of Hurricane Katrina and received more than $33,000 in benefits from the Federal Emergency Management Agency (FEMA), Red Cross, and other organizations. During this reporting period, the senior correctional officer was sentenced in the Western District of Louisiana to 16 months' incarceration followed by 3 years' supervised release pursuant to his jury-trial conviction on charges of theft of public money, wire fraud, and making false statements. In addition, he was ordered to pay FEMA $22,540 in restitution, pay a $1,000 fine, and perform 100 hours of community service.

- An investigation by the OIG's Houston Area Office led to the arrest and conviction of a BOP correctional officer on charges of bribery. OIG investigators determined that on four occasions the correctional officer accepted bribes totaling $3,600 from an inmate in exchange for smuggling tobacco into the Federal Correction Institution. Sentencing is pending.

- An investigation by the OIG's Washington Field Office led to the arrest of a senior BOP correctional officer on charges of deprivation of rights under the color of law and making a false statement. Investigators determined that the senior correctional officer assaulted two

inmates by closing a steel food-tray door on their arms and provided a false statement about the incidents to the OIG. Judicial proceedings continue.

Ongoing Work

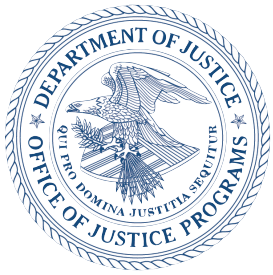
The BOP's Administration of the Witness Security Program

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

Review of Health and Safety Issues at BOP Computer Recycling Facilities

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

Office of Justice Programs



OJP manages the majority of the Department's grant programs and is responsible for developing initiatives to address crime at the state and local level. OJP has a personnel ceiling of 697 positions and is composed of 5 bureaus – Bureau of Justice Assistance (BJA), Bureau of Justice Statistics, National Institute of Justice (NIJ), Office of Juvenile Justice and Delinquency Prevention, and Office for Victims of Crime (OVC) – as well as the Community Capacity Development Office and the Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking Office.

Reports Issued

Hometown Heroes Survivors Benefits

The OIG's Evaluation and Inspections Division reviewed OJP's implementation of the *Hometown Heroes Survivors Benefits Act of 2003* (Hometown Heroes Act). This review was in response to Congressional concerns that OJP took too long to process claims submitted under the Act and that OJP's narrow interpretation of terms found in the Act was causing a high rate of claims denials.

BJA manages Hometown Heroes Act claims as part of its Public Safety Officers' Benefits Program, which provides death and educational assistance benefits to survivors of public safety officers who died and disability benefits to officers injured in the line of duty. The Hometown Heroes Act expanded the benefits program to include benefits for deaths from heart attacks or strokes that occur in the line of duty or within 24 hours of a triggering effect while on duty. The Act also included a statutory presumption that public safety officers who died from a heart attack or stroke following a "nonroutine stressful or strenuous" physical public safety activity or training died in the line of duty for the program's purposes.

Our evaluation found that as of November 29, 2007, OJP had completed only half of the Hometown Heroes Act claims it received in the first 3 years after the Act's passage. One reason for the delay in processing claims was that OJP took 33 months to issue final regulations implementing the Act. During that time, OJP developed a backlog of 201 claims. After OJP issued the necessary regulations in September 2006, it processed claims slowly because: 1) most claims had been submitted without required documentation, 2) its Office of the General Counsel's legal reviews of claims were time consuming, and 3) decisions on some claims were delayed because OJP could not obtain necessary pathology reviews. In late 2007, OJP implemented

several initiatives designed to expedite its processing of claims and, by the end of our review, had reduced the backlog of claims to 99. In March 2008, the backlog had been reduced to 27 claims.

We also found that OJP initially denied some claims based in part on its narrow legal interpretation of the definition of "nonroutine" activities. In October 2007, BJA issued policy memoranda clarifying that any response to an emergency call should be considered "nonroutine" for purposes of analyzing claims under the Act. The Director of the Public Safety Officers' Benefits Program Office stated that this step has led to more claims being approved and faster claims processing.

The OIG recommended that OJP finalize a guide to the Hometown Heroes Act directed to claimants, have its Office of the General Counsel establish more definitive timeliness standards for its legal reviews of claims, and use a new case management system to expedite processing of claims. OJP agreed with our recommendations.

The Paul Coverdell Forensic Science Improvement Grants Program

In January 2008, the OIG's Evaluation and Inspections Division released a follow-up report examining OJP's Paul Coverdell Forensic Science Improvement Grants Program. Coverdell grants are awarded to state and local governments to improve the timeliness and quality of their forensic science and medical examiner services and to eliminate backlogs in the analysis of DNA and other forensic evidence. One condition of receiving a Coverdell grant is the grantee must certify that an entity exists and an appropriate process is in place to conduct independent external investigations into allegations of serious negligence or misconduct. This requirement was implemented to address allegations of forensic laboratory negligence, misconduct, and false testimony by forensic laboratory staff that have led to wrongful convictions in several states.

A December 2005 OIG report concluded that OJP was not effectively administering the certification requirement because it had not required grant applicants to identify the names of the certified government entities. Our latest review, issued in January 2008, examined OJP's administration of the Coverdell independent investigation certification requirement and found that, even though OJP has obtained certifications from grant applicants, it has not ensured that applicants certify entities that are qualified to conduct independent investigations of the forensics laboratories and has not required that allegations be appropriately referred for investigation. We also found that, while OJP had started requiring applicants to provide the name of the government entity, OJP still was not ensuring that applicants named entities that were actually capable of conducting independent investigations of alleged wrongdoing.

The OIG review found that one-third of the named entities lacked the authority, capabilities and resources, or an appropriate process to conduct independent external investigations into allegations of serious negligence or misconduct. In addition, several certifying officials told the OIG that when they completed the certification they did not have a specific entity in mind and merely signed the document OJP provided. We also found that OJP did not provide adequate guidance to ensure that grantees and forensic laboratories actually referred allegations of negligence and misconduct to the certified government entities for investigation.

The OIG made three recommendations to improve the effectiveness of OJP's grant administration

and better ensure that serious allegations of negligence or misconduct are referred for independent investigations. OJP concurred with recommendations that it provide guidance to refer allegations to certified government entities and to revise and document its application review process. OJP did not agree with the recommendation to require applicants to name the government entities and confirm that the entities have the authority, independence, and the resources to conduct independent, external investigations.

The Southwest Border Prosecution Initiative Reimbursement Program

The OIG's Audit Division audited the Southwest Border Prosecution Initiative (SWBPI), a $30 million annual program administered by OJP through which the Department provides reimbursement to four Southwest Border states and local jurisdictions for the prosecution and pre-trial detention costs in federally initiated cases that are declined by the USAO.

We found several deficiencies in OJP's oversight of the SWBPI program. From October 1, 2001, through September 31, 2006, OJP provided $161 million in reimbursement to four Southwest Border states and local jurisdictions. In seven audits of individual jurisdictions who received this funding, we found $15.7 million in questioned costs, which represented 28 percent of the total $55 million in reimbursements that we audited. We also found that OJP does not require applicants to provide documentation supporting reimbursement requests, does not review the applications for accuracy, and does not monitor recipients to determine the eligibility of cases submitted for reimbursement. In our judgment, most of the unallowable and unsupported reimbursements we identified could have been avoided if OJP required applicants to submit supporting documents.

On every SWBPI reimbursement application, the jurisdiction's Chief Executive Officer (CEO) or designee must certify that the SWBPI claim, combined with other federal funding, does not exceed 100 percent of the cost of prosecuting and detaining defendants during the reporting period. However, we found that reimbursements are not linked to actual costs incurred by the jurisdictions to prosecute federally declined criminal cases. Moreover, none of the seven jurisdictions included in our audit maintained any documentation to support the costs submitted for reimbursement that were associated with SWBPI cases. This resulted in reimbursements totaling $49.78 million that could not be linked to actual costs incurred by the jurisdictions to prosecute federally declined criminal cases.

Additionally, on every SWBPI reimbursement application the jurisdiction's CEO or designee is required to certify that the SWBPI claim has been adjusted to account for additional prosecution and pre-trial detention funding received through other federal programs. We found that six of the seven state and local jurisdictions included in our audit did not take any steps to ensure that the SWBPI reimbursements, when combined with additional federal funding, did not exceed the cost to prosecute the SWBPI cases. This failure could result in jurisdictions being reimbursed by the federal government more than once for the same prosecutions and pre-trial detention services.

We made 13 recommendations regarding OJP's oversight of the SWBPI. OJP agreed with our recommendations.

Audits of OJP Grants to State and Local Entities

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

- We found that the city and county of San Francisco, California, which received more than $5.4 million in SWBPI funding, claimed and received unallowable reimbursements for the 2,241 cases submitted that were not initiated by a federal law enforcement agency or task force in accordance with SWBPI guidelines. We questioned the reimbursements for the total amount of $5.4 million that San Francisco received. OJP agreed with our recommendation to remedy the more than $5.4 million in questioned costs.

- We found that Brooks County, Texas, which received more than $7.8 million in SWBPI funding, claimed and was reimbursed for unsupported cases and cases that were ineligible under SWBPI guidelines. Based on unallowable and unsupported costs, we identified questioned costs of more than $1.9 million.

- BJA awarded a Community Justice Empowerment Project grant totaling approximately $3.16 million to the National Training and Information Center (NTIC) in Chicago, Illinois, to provide training, technical assistance, and funding to community-based organizations. More than half the grant funds were awarded to subgrantees who were to be competitively selected on their ability to run a successful community program. However, evidence in the grantee's files and statements by NTIC staff revealed that the majority of subgrantees were instead selected based upon their connection to influential lawmakers. Moreover, while a major element of the grant was to provide training to the subgrantees and significant funds were spent for training conferences, considerable portions of these sessions were dedicated to conducting congressional lobbying visits and training subgrantees on how to conduct successful lobbying activities.

  In addition, we found inadequate controls over expenditures, unallowable personnel costs, improper and unallowable non-personnel costs, and contractor irregularities, and we questioned the entire grant amount. We made 37 recommendations to OJP to address the deficiencies we identified during our audit. OJP agreed with our recommendations and suspended funding to NTIC.

  The OIG's Investigations Division initiated a criminal investigation related to this grant. As a result, the NTIC Executive Director was arrested, pled guilty, and served a sentence for misuse of federal program funds. A civil complaint pursuant to the *False Claims Act* has also been filed in the Northern District of Illinois.

Investigations

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

- In our March 2007 *Semiannual Report to Congress*, we reported on a joint investigation by the OIG's San Francisco Area Investigations and Audit Offices, FBI, Department of

Housing and Urban Development (HUD), and Internal Revenue Service that led to the arrest of the former Mayor of Fairbanks, Alaska, and his wife on charges of theft of $450,000 in federal grant funds, conspiracy, and money laundering. The investigation developed evidence that the former Mayor and his wife used grant funds from OJP and HUD that were designated to operate a non-profit organization to purchase a flat screen television and other items for personal use and to partially fund the building of their church. During this reporting period, the former Mayor was convicted on 16 counts of theft of government funds, conspiracy, money laundering, and submitting false tax returns, while his wife pled guilty to charges of money laundering and theft of federal funds. Sentencing is scheduled for May 2008.

- A joint investigation by the OIG's Chicago Field Office and the FBI led the arrest and guilty plea of a Department grantee on charges of theft of program funds. The investigation determined that the grantee, while serving as ombudsman for the Putnam County Sheriff's Department in Indiana, stole $57,916 in BJA grant funds and $30,914 in general funds belonging to the Sheriff's Department. The grantee had applied for the federal grant funds without the knowledge of county officials, then withdrew the funds from a special projects account and deposited them into his personal bank accounts. The grantee used the funds for personal expenditures, including jewelry, clothing, furniture, and a trip to Florida. He was sentenced in the Southern District of Indiana to 18 months' incarceration followed by 3 years' supervised release. He also was ordered to pay restitution to the Department and the Putnam County Sheriff's Department.

Ongoing Work

Management of the Grant Program for Human Trafficking Victims

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

NIJ's Grant and Contract Award Practices

As required by the *Consolidated Appropriations Act of 2008*, the OIG is examining contracts and grants awarded by the NIJ in the last 3 fiscal years, including the competition for these grants and the potential for conflicts of interest in the awards process.

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 10,800 employees staffing its 23 division offices in the United States and the Caribbean and 86 offices in 62 other countries.

Reports Issued

The DEA's Controls over Weapons and Laptop Computers

The OIG's Audit Division examined whether the DEA has addressed weaknesses in its control over its weapons and laptop computers, including purchasing, disposing, transferring custodianship, identifying laptop contents, and conducting physical inventories. These weaknesses were reported in a 2002 OIG audit.

The follow-up review, which examined activity from January 2002 through June 2007, found that the DEA's rate of loss for weapons has increased since our 2002 review, while the DEA's rate of loss for laptop computers during the same period has declined. From January 2002 through June 2007, 91 DEA weapons and 231 laptop computers were lost or stolen, compared with 16 weapons and 229 laptop computers lost or stolen during the 26-month period covered in our 2002 audit.

Our review also found that the DEA could not determine what information was on its lost or stolen laptop computers, and it was unable to provide assurance that 226 of the 231 lost or stolen laptop computers did not contain sensitive or personally identifiable information. Moreover, few of the laptops lost or stolen during our review period were protected by encryption software because the DEA did not begin installing such software on its laptops until November 2006.

We determined that the DEA has made improvements to its internal controls over weapons and laptop computers since our 2002 audit, such as conducting physical inventories and reconciling these inventories to its financial system records. However, the DEA still requires significant improvement in its overall controls on weapons and laptops. For example, DEA employees were not internally reporting lost or stolen weapons and laptops in a timely manner. Further, the DEA was not informing the Department of weapon and laptop losses, and the DEA was not ensuring that relevant information about lost weapons and laptops was entered in the National Crime Information Center (NCIC) database, thereby hindering the chances of recovering the lost property.

The OIG report made seven recommendations, including that the DEA ensure that its employees accurately and promptly report weapon and laptop losses to DEA headquarters and other appropriate components, require encryption software on all laptop computers, ensure the accurate and timely entry of weapon and laptop losses in the NCIC database, and require that the investigation of lost laptops include a determination of the laptop's contents. The DEA agreed with all of the recommendations except the recommendation to require encryption software on all laptop computers.

The DEA's Diversion Control Fee Account

The OIG's Evaluation and Inspections Division reviewed whether the DEA used Diversion Control Fee Account (Fee Account) funds for activities that were unrelated to the diversion of controlled pharmaceuticals. Controlled pharmaceuticals, such as narcotics, stimulants, and depressants, can be diverted from legitimate channels through theft or fraud during the manufacturing and distribution process. They also can be diverted by medical staff, pharmacy staff, and individuals involved in selling or using pharmaceuticals. The DEA is required by statute to fund its efforts to investigate the diversion of controlled pharmaceuticals through registration fees that manufacturers, distributors, physicians, and others pay into the Fee Account.

The OIG review examined allegations that the DEA may have used funds from the Fee Account to pay for non-diversion activities. Our review did not substantiate the allegations that the DEA misused funds from the account during the period reviewed, FY 2004 through FY 2007.

However, our review concluded that the DEA did not fully fund all of its diversion control salary costs that were directly related to Diversion Control Program activities with the Fee Account, as required by law. For example, in FYs 2006 and 2007 the DEA paid approximately $15.4 million in salary costs of special agents and chemists working on criminal diversion investigations with appropriated funds rather than with funds from the Fee Account.

The OIG recommended that the DEA determine both the actual and planned costs attributable to diversion control activities, especially those for special agents, intelligence analysts, and chemists, and include these costs in the Diversion Control Program's future budgets. The OIG also recommended that the DEA provide more information to its personnel on the requirements that govern the use of Fee Account funds. The DEA concurred with both recommendations.

Ongoing Work

The DEA's Utilization of Intelligence Analysts and Reports Officers

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

U.S. Marshals Service

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

Investigations

During this reporting period, the OIG received 163 complaints involving the USMS. The most common allegations made against USMS employees included job performance failure, official misconduct and force, abuse, and rights violations. The OIG opened 10 investigations and referred other allegations to the USMS's Office of Internal Affairs for review.

At the close of the reporting period, the OIG had 22 open cases of alleged misconduct against USMS employees. The following is an example of a case involving the USMS that the OIG's Investigations Division handled during this reporting period:

- An investigation by the OIG's San Francisco Area Office led to the arrest and guilty plea of a USMS supervisory deputy marshal on a charge of making a false statement. The investigation determined that the supervisory deputy marshal submitted an application for promotion to the USMS in which he falsely claimed he had a 4-year degree from a university and included false transcripts with the application. When interviewed, the supervisory deputy marshal admitted he purchased the degree and transcripts online from a "diploma mill" for $703. He subsequently retired from the USMS. Sentencing is pending.

Bureau of Alcohol, Tobacco, Firearms and Explosives

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

Ongoing Work

ATF's Controls Over Weapons and Laptops and Other Sensitive Property

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

Other Department Components

U.S. Attorneys' Offices

U.S. attorneys serve as the federal government's principal criminal and civil litigators and conduct most of the trial work in which the United States is a party. Under the direction of the Attorney General, 94 U.S. attorneys are stationed throughout the United States, Puerto Rico, U.S. Virgin Islands, Guam, and Northern Mariana Islands. More than 11,200 employees work in those offices and in the EOUSA.

Reports Issued

The Department's Victim Notification System

The OIG's Audit Division issued an audit of the Department's Victim Notification System (VNS), an automated system managed by EOUSA that notifies federal crime victims regarding developments in their cases, including information about the status of the investigation, prosecution, trial, and incarceration of the offender related to the crime. Victims in the VNS are notified by letter, e-mail, facsimile, or telephone when a particular event in a case occurs, such as a scheduled court date or the release of a prisoner. As of October 5, 2007, the VNS contained information on more than 1.5 million registered victims.

As part of this review, the OIG conducted surveys of active and inactive crime victims in the VNS and found that, overall, survey respondents generally were satisfied with VNS services. We found that victims generally believed VNS notifications were understandable and useful, obtained information they wanted from the VNS Call Center, and were able to easily navigate the VNS website.

However, the surveys also identified areas in which improvements could be made. A quarter of survey respondents indicated that they had not heard of the VNS prior to receiving the OIG's survey, had never received a notification from the VNS, or were not aware that they were registered as crime victims in the VNS. In addition, while the OIG surveys revealed that more than 70 percent of respondents considered the custody status of offenders involved in their cases to be an important piece of information, this information is not consistently entered into the VNS. In addition, 56 percent of victims responding to the survey indicated that they were dissatisfied with the amount of information available to them through the VNS regarding restitution.

We found few internal controls in place to ensure the accuracy and completeness of data in the VNS. We also identified deficiencies in the security of VNS information, most notably that the sensitive crime victim information contained within the

VNS was not adequately protected against loss of confidentiality and that the integrity and availability of data was not appropriately ensured.

The OIG made 19 recommendations to help improve EOUSA's management of the VNS, such as developing an interface to connect all relevant federal agencies to the VNS, formalizing long-term plans for the system and its management, improving certain facets of Call Center services, and addressing the vulnerabilities identified during the information security review of the VNS. EOUSA concurred with our recommendations and has outlined a plan to address them.

Investigations

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

- An investigation by the OIG's New York Field Office, with assistance from the Department of Housing and Urban Development (HUD) OIG, led to the arrest of a USAO legal assistant on charges of fraud and making false statements. The investigation determined that between 1985 and 2006 the legal assistant received federal housing benefits estimated at $137,993. The legal assistant submitted fraudulent pay statements to support her claim and failed to disclose the extent of her federal employment income from the USAO. Judicial proceedings continue.

Ongoing Work

Review of USAOs' Resource Management

The OIG is auditing the allocation of resources of the 94 USAOs. In particular, the audit is examining the allocation and utilization of federal prosecutors within USAOs, the accuracy and completeness of USAO utilization and casework data, and the type and number of cases being handled by the USAOs.

Executive Office for U.S. Trustees

Reports Issued

The U.S. Trustee Program's Oversight of Chapter 7 Panel Trustees and Debtors

The OIG's Audit Division evaluated the effectiveness of the U.S. Trustee Program (USTP) in monitoring the performance of Chapter 7 panel trustees. The USTP is responsible for supervising the administration of bankruptcy cases and trustees, including Chapter 7 panel trustees. The USTP appoints over 1,000 Chapter 7 panel trustees nationwide who are responsible for collecting over $2 billion in funds annually through the liquidation of debtors' estates and distributing those funds to secured and unsecured

creditors in accordance with the U.S. Bankruptcy Code.

Our audit report, which examined the USTP's monitoring of panel trustees from FYs 2004 through 2007, found that the procedural framework of audits and reviews established by the USTP was adequate to ensure the competency and integrity of panel trustees in discharging their fiduciary duties. However, we found that field examinations of panel trustee operations – one of the USTP's primary oversight mechanisms – were not conducted within the required 4-year timeframe for 26 percent of the trustees requiring field examinations during the review period. In several instances, field examinations were not conducted at all, which resulted in some panel trustees being allowed to operate for 8 years without an on-site review of their operations.

USTP staff also are supposed to conduct annual reviews of trustees' interim reports. Of the 156 trustee interim reports that we reviewed in a judgmental sample, we found that 18 percent of the reviews were not conducted or adequately documented. Not consistently examining these reports on a timely basis could increase the risk that a panel trustee's poor performance or misconduct may go undetected.

We provided four recommendations for the improvement of the USTP's oversight efforts. The Department concurred with our recommendations.

Criminal Division

Reports Issued

Equitable Sharing Audits

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

During this reporting period, the OIG's Audit Division audited the Douglas County Sheriff's Office (DCSO) in Omaha, Nebraska, and reviewed the DCSO's compliance with six essential equitable sharing guidelines.

The Department awarded the DCSO with equitable sharing revenues totaling nearly $1.3 million and property valued at $64,929 to support law enforcement operations. We found that the DCSO complied with the equitable sharing guidelines with respect to use of equitable sharing property, interest earned on equitable sharing funds, and non-supplanting requirements. However, we identified weaknesses related to the DCSO's: 1) Federal Sharing Agreements and Annual Certification Reports, 2) accounting for equitable sharing receipts, and 3) use of equitable sharing funds. We made five recommendations, including requiring the DCSO to resubmit the FY 2006 and 2007 Annual Certification Reports with corrected information and accurately account for equitable sharing receipts. The DCSO agreed with our recommendations.

Top Management and Performance Challenges

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

The OIG's current list of top challenges, issued in November 2007, is presented to the right. The challenges are not listed in order of priority – we believe that all are critical management and performance issues facing the Department. However, it is clear that the top challenge facing the Department is its ongoing response to the threat of terrorism. Several other top challenges are closely related to and impact directly on the Department's counterterrorism efforts.

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

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

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

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

Congressional Testimony

On October 24, 2007, the Inspector General testified before the Senate Committee on Homeland Security and Governmental Affairs about the operations of the Terrorist Screening Center.

On November 8, 2007, the Inspector General also testified before the House Committee on Homeland Security on the operations of the Terrorist Screening Center.

On January 23, 2008, the Inspector General testified before the Senate Committee on the Judiciary on oversight of the Department's forensic grant programs.

Legislation and Regulations

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

During this reporting period, the OIG commented on proposed legislation in the Senate that would amend the IG Act to strengthen the independence and accountability of Inspectors General. The Senate bill is a companion bill to legislation passed by the House of Representatives on October 3, 2007.

In particular, the OIG supports a provision in the legislation that would remove the limitation on the OIG's jurisdiction within the Department. Unlike all other federal Inspectors General who are authorized to investigate misconduct throughout their entire agencies, the OIG does not have the authority to investigate allegations against Department attorneys acting in their legal capacity, including allegations against the Attorney General or Deputy Attorney General. Instead, the Department's Office of Professional Responsibility has jurisdiction to investigate such allegations. The OIG believes the limitation on its jurisdiction should be removed because it creates conflicts of interest, results in duplicative and overlapping investigations, prevents the OIG from addressing systemic issues involving Department conduct, and contravenes the rationale for establishing Inspectors General throughout the government.

Statistical Information

Audit Statistics

Audit Summary

During this reporting period, the OIG's Audit Division issued 137 audit reports containing more than $20.8 million in questioned costs and more than $174,000 in funds to be put to better use and made 322 recommendations for management improvement. Specifically, the Audit Division issued 22 internal audit reports of Department programs funded at more than $887 million; 40 external audit reports of contracts, grants, and other agreements funded at more than $84 million; and 75 *Single Audit Act* audits. In addition, the Audit Division issued nine Notifications of Irregularities and one Technical Assistance Memorandum.

Funds Recommended to Be Put to Better Use

Audit Reports	Number of Audit Reports	Funds Recommended to Be Put to Better Use
No management decision made by beginning of period	3	$3,051,384
Issued during period	2	$174,807
Needing management decision during period	5	$3,226,191
Management decisions made during period:		
◆ Amounts management agreed to put to better use[1]	2	$174,807
◆ Amounts management disagreed to put to better use	0	$0
No management decision at end of period	3	$3,051,384

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

Audits with Questioned Costs

Audit Reports	Number of Audit Reports	Total Questioned Costs (including unsupported costs)	Unsupported Costs
No management decision made by beginning of period	7	$8,890,694	$3,165,274
Issued during period	42	$20,865,895	$10,355,920
Needing management decision during period	49	$29,756,589	$13,521,194
Management decisions made during period:			
◆ Amount of disallowed costs[1]	32[2]	$21,509,444	$11,264,438
◆ Amount of costs not disallowed	0	$0	$0
No management decision at end of period	18	$8,247,145	$2,256,756

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

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

Audits Involving Recommendations for Management Improvements

Audit Reports	Number of Audit Reports	Total Number of Management Improvements Recommended
No management decision made by beginning of period	14	34
Issued during period	91	329
Needing management decision during period	105	363
Management decisions made during period:		
◆ Number management agreed to implement[1]	86[2]	300
◆ Number management disagreed with	0	0
No management decision at end of period	21	63

[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 two 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.

National Defense Authorization Act

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

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

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

Audit Follow-up

OMB Circular A-50

OMB Circular A-50, *Audit Followup*, 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, 2008, the OIG has closed 127 audit reports and was monitoring the resolution process of 353 open audit reports.

Unresolved Audits

Audits Over 6 Months Old without Management Decisions

As of March 31, 2008, the following audits had no management decision or were in disagreement:

- Office of Community Oriented Policing Services Grants to the Passamaquoddy Tribe and Pleasant Point Reservation Police Department, Perry, Maine
- Oversight of Intergovernmental Agreements by the USMS and the Office of the Federal Detention Trustee
- USMS Intergovernmental Service Agreement for Detention Facilities with the Blount County, Tennessee, Sheriff's Office
- USMS Intergovernmental Service Agreement for Detention Facilities with the Central Virginia Regional Jail
- USMS Intergovernmental Service Agreement for Detention Facilities with the Cumberland County Jail, Portland, Maine
- USMS Intergovernmental Service Agreement for Detention Facilities with the Dona Ana County Detention Center, Las Cruces, New Mexico
- USMS Intergovernmental Service Agreement for Detention Facilities with the Hamilton County, Tennessee, Silverdale Correctional Facility
- USMS Intergovernmental Service Agreement for Detention Facilities with the Western Tidewater Regional Jail, Suffolk, Virginia
- Use of Equitable Sharing of Revenues by the Fayette County, Georgia, 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, 2008.

E&I Workload Accomplishments	Number of Reviews
Reviews active at beginning of period	6
Reviews initiated	3
Final reports issued	5
Reviews active at end of reporting period	4

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, 2008, one report, "The United States Marshals Service Judicial Security Process," had two unresolved recommendations. The OIG continues to work with the USMS to resolve it.

Investigations Statistics

The following chart summarizes the workload and accomplishments of the Investigations Division during the 6-month period ending March 31, 2008.

Source of Allegations	
Hotline (telephone and mail)	149
Other sources	4,481
Total allegations received	4,630
Investigative Caseload	
Investigations opened this period	180
Investigations closed this period	161
Investigations in progress as of 3/31/08	413
Prosecutive Actions	
Criminal indictments/ informations	53
Arrests	56
Convictions/Pleas	69
Administrative Actions	
Terminations	16
Resignations	64
Disciplinary action	28
Monetary Results	
Fines/Restitutions/Recoveries	$4.7 million
Seizures	$81,495
Bribe monies deposited to the Treasury	$4,700

Integrity Awareness Briefings

OIG investigators conducted 155 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 5,400 employees.

Appendix 1

Acronyms and Abbreviations

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

ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
BOP	Federal Bureau of Prisons
BJA	Bureau of Justice Assistance
CODIS	Combined DNA Index System
DEA	Drug Enforcement Administration
Department	U.S. Department of Justice
DHS	Department of Homeland Security
EOUSA	Executive Office for U.S. Attorneys
FBI	Federal Bureau of Investigation
FY	Fiscal year
IG Act	*Inspector General Act of 1978*
IT	Information technology
NIJ	National Institute of Justice
NSL	National Security Letters
OIG	Office of the Inspector General
OJP	Office of Justice Programs
OVC	Office for Victims of Crime
Patriot Reauthorization Act	*USA Patriot Improvement and Reauthorization Act of 2005*
UNICOR	Federal Prison Industries, Inc.
USAO	U.S. Attorneys' Offices
USMS	U.S. Marshals Service

Appendix 2

Glossary of Terms

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

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

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

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

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

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

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

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

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

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

Appendix 3

Evaluation and Inspections Division Reports

October 1, 2007 – March 31, 2008

Review of OJP's Paul Coverdell Forensic Science Improvement Grants Program

Review of the DEA's Use of the Diversion Control Fee Account

Review of the FBI's Use of NSLs: Assessment of Corrective Actions and Examination of NSL Usage in 2006 (joint effort with Oversight and Review Division)

Review of the FBI's Use of Section 215 Orders for Business Records in 2006 (joint effort with Oversight and Review Division)

OJP's Implementation of the *Hometown Heroes Survivors Benefits Act of 2003*

Appendix 4

Audit Division Reports

October 1, 2007 – March 31, 2008

INTERNAL AND EXTERNAL AUDIT REPORTS

Annual Accounting and Authentication of Drug Control Funds and Related Performance FY 2007

Assets Forfeiture Fund and Seized Asset Deposit Fund Annual Financial Statement FY 2007

Audit of the Department's Key Indicators

Audit of the Department's Terrorist Watchlist Nomination Processes

ATF's Annual Financial Statement FY 2007

Compliance with Standards Governing Combined DNA Index System Activities at the Palm Beach County Sheriff's Office Crime Laboratory, West Palm Beach, Florida

Compliance with Standards Governing Combined DNA Index System Activities at the Indiana State Police Laboratory, Indianapolis, Indiana

Compliance with Standards Governing Combined DNA Index System Activities at the Tulsa Police Department Forensic Laboratory, Tulsa, Oklahoma

Compliance with Standards Governing Combined DNA Index System Activities at the Texas Department of Public Safety Crime Laboratory, Waco, Texas

Compliance with Standards Governing Combined DNA Index System Activities at the Utah Department of Public Safety, Bureau of Forensic Services, Salt Lake City, Utah

The DEA's Annual Financial Statement FY 2007

The FBI's Annual Financial Statement FY 2007

The BOP's Annual Financial Statement FY 2007

Federal Prison Industries, Inc., Annual Financial Statement FY 2007

Implementation of the *Communications Assistance for Law Enforcement Act* by the FBI

OJP's Annual Financial Statement FY 2007

OJP Grants Awarded to the Washington Department of Corrections, Olympia, Washington

OJP San Diego Region Anti-Trafficking Task Force Grant Awarded to the County of San Diego, California

OJP Southwest Border Prosecution Initiative Funding Received by the City and County of San Francisco, California

OJP Southwest Border Prosecution Initiative Funding Received by Brooks County, Texas

OJP State and Local Emergency Preparedness Grant Awarded to the Maryland Department of State Police

OJP BJA Community Justice Empowerment Project Grant Administered by the National Training and Information Center, Chicago, Illinois

OJP BJA Grant Awarded to the 7th Judicial Administrative District, State of Georgia for the Tallapoosa Drug Intervention Program, Cartersville, Georgia

OJP BJA Grant Awarded to the City and County of Denver, Colorado

OJP BJA Tribal Drug Courts Grants Awarded to the Crow Tribe of Indians Crow Agency, Montana

OJP NIJ Cooperative Agreement Awarded to North Dakota State University, Fargo, North Dakota

OJP Office of Juvenile Justice and Delinquency Prevention Grant Administered by the Boys and Girls Home Residential Treatment Center, Inc., Sioux City, Iowa

OJP OVC Grants Administered by the Illinois Court of Claims, Springfield, Illinois

OJP OVC Services for Trafficking Victims Discretionary Grant Program, Cooperative Agreement Awarded to the International Rescue Committee, New York, New York

OJP Office of Violence Against Women Legal Assistance for Victims Grant and Services for Human Trafficking Victims Grants Administered by the Heartland Alliance for Human Needs and Human Rights, Chicago, Illinois

Offices, Boards and Divisions Annual Financial Statement FY 2007

Review of the FBI Headquarters' Information System Controls Environment FY 2007

Review of the Department's Consolidated Information System General Controls Environment FY 2007

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Public Allies, Inc., Milwaukee, Wisconsin

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Mayor's Time, Inc., Detroit, Michigan

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Legal Actions of Wisconsin, Inc., Milwaukee, Wisconsin

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Washtenaw County Juvenile Drug Court Implementation Program, Ann Arbor, Michigan

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Oklahoma Coalition Against Domestic Violence and Sexual Assault

Survey of Internal Control Procedures Over Department Grant Funds Administered by the City of Lawton, Oklahoma

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Women's Shelter, Inc.

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Women Together Foundation, Inc.

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Bitter Root RC&D Area, Inc.

Survey of Internal Control Procedures Over Department Grant Funds Administered by the City of Espanola, New Mexico

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Hopi Tribe, Arizona

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Builders for Family and Youth of the Diocese of Brooklyn

Survey of Internal Control Procedures Over Department Grant Funds Administered by the First State Community Action Agency

Survey of Internal Control Procedures Over Department Grant Funds Administered by the Megan Nicole Kanka Foundation, Trenton, New Jersey

Survey of Internal Control Procedures Over Department Grant Funds Administered by the City of Maywood, California

Survey of Internal Control Procedures Over Department Grant Funds Administered by the SAGE Project, Inc., San Francisco, California

Survey of Internal Control Procedures Over Department Grant Funds Administered by the National Academy of Sciences, Washington, D.C.

Survey of Internal Control Procedures Over Department Grant Funds Administered by BRTRC, Inc., Fairfax, Virginia

Survey of Internal Control Procedures Over Handling of Receipts for Department Grant Awarded to the Athens Clarke County, Georgia, Driving Under the Influence/Drug Court

Survey of Internal Control Procedures Over the Administration of Department of Justice Grants Sub-Awarded by the Puerto Rico Department of Justice to Carlos Albizu University, San Juan, Puerto Rico

The Department's Annual Financial Statement FY 2007

The Department's Victim Notification System

The DEA's Controls Over Weapons and Laptop Computers Follow-up Audit

The FBI's Management of Confidential Case Funds and Telecommunication Costs

The BOP's Efforts to Manage Inmate Health Care

The Southwest Border Prosecution Initiative Reimbursement Program

The U.S. Trustee Program's Oversight of Chapter 7 Panel Trustees and Debtors

The USMS's Annual Financial Statement FY 2007

Use of Equitable Sharing Revenues by the Douglas County Sheriff's Office, Omaha, Nebraska

Single Audit Act Reports of Department Activities

October 1, 2007 – March 31, 2008

Apsaalooke Nation Housing Authority, Crow Agency, Montana

Asotin County, Asotin, Washington

Bright Horizons Resources for Survivors of Domestic Violence and Sexual Assault, Norfolk, Nebraska

Brown County, Nashville, Indiana

Caldwell County, Kingston, Missouri

Champaign County, Urbana, Ohio

City of Baltimore, Maryland

City of Bastrop, Louisiana

City of Boonville, Missouri

City of Chula Vista, California

City of Cincinnati, Ohio

City of Gary, Indiana

City of Harrisburg, Pennsylvania

City of Indianapolis, Indiana

City of Kansas City, Missouri

City of Lake Charles, Louisiana

City of Montgomery, Minnesota

City of Newark, Delaware

City of Portsmouth, New Hampshire

City of San Diego, California

City of Scranton, Pennsylvania

City of South El Monte, California

City of Visalia, California

Clay County, Spencer, Iowa

Colorado Coalition Against Domestic Violence, Denver, Colorado

Confederated Tribes of the Colville Reservation, Nespelem, Washington

Crow Tribe of Indians, Crow Agency, Montana

Domestic Violence Intervention Services, Inc., Tulsa, Oklahoma

Florida Council Against Sexual Violence, Tallahassee, Florida

Franklin County, Columbus, Ohio

Greene County, Springfield, Missouri

Hall County, Grand Island, Nebraska

Hawaii Community Foundation, Honolulu, Hawaii

Howell County, West Plains, Missouri

Indian Township Tribal Government, Princeton, Maine

Itasca County, Grand Rapids, Minnesota

Johnson County, Warrensburg, Missouri

Kanawha County, Charleston, West Virginia

Kickapoo Tribe of Oklahoma, McLoud, Oklahoma

Lake County, Polson, Montana

Levy County, Bronson, Florida

Marion County, Marion, South Carolina

Marshall County Commission, Guntersville, Alabama

Mescalero Apache Tribe, Mescalero, New Mexico

Miami/Miami-Dade Weed and Seed, Inc., Miami, Florida

Minnesota Program Development, Inc., Duluth, Minnesota

Mississippi County, Charleston, Missouri

Montgomery County, Independence, Kansas

Municipality of Corozal, Puerto Rico

Northern Cheyenne Tribe, Lame Deer, Montana

Northwest Crime and Social Research, Inc., Olympia, Washington

Pulaski County, Waynesville, Missouri

Southwest Center for Law and Policy, Inc., Tucson, Arizona

St. Louis County, St. Louis, Missouri

State of Connecticut, Hartford, Connecticut

State of Hawaii Department of Public Safety, Honolulu, Hawaii

State of Louisiana, Baton Rouge, Louisiana

State of Nebraska, Lincoln, Nebraska

State of North Dakota, Bismarck, North Dakota

State of Ohio, Columbus, Ohio

State of South Carolina, Columbia, South Carolina

State of Washington, Olympia, Washington

Tangipahoa Parish Sheriff, Amite, Louisiana

The Navaho Nation, Window Rock, Arizona

Town of Brattleboro, Vermont

Town of Davie, Florida

Township of Muhlenberg, Pennsylvania

University of Missouri, Columbia, Missouri

University of Notre Dame, Notre Dame, Indiana

University of Toledo, Toledo, Ohio

Verde Valley Sanctuary, Inc., Sedona, Arizona

Washington Association of Sheriffs and Police Chiefs, Lacey, Washington

Whatcom County, Bellingham, Washington

Yellowstone Boys & Girls Ranch, Billings, Montana

YWCA of Lewiston-Clarkston, Lewiston, Idaho

Audit Division Reports

October 1, 2007 – March 31, 2008

Quantifiable Potential Monetary Benefits			
Audit Report	**Questioned Costs**	**Unsupported Costs**	**Funds Put to Better Use**
Apsaalooke Nation Housing Authority, Crow Agency, Montana	$9,250	$9,250	
Asotin County, Asotin, Washington	$165,170	$165,170	
City of Boonville, Missouri	$1,354	$1,354	
City of Chula Vista, California	$38,961		
City of Cincinnati, Ohio	$98,995		
City of Kansas City, Missouri	$89,667	$89,667	
City of Lake Charles, Louisiana	$34,285	$34,285	
City of San Diego, California	$14,945	$14,945	
Colorado Coalition Against Domestic Violence, Denver, Colorado	$1,875	$1,875	
Franklin County, Columbus, Ohio	$74,230		
Itasca County, Grand Rapids, Minnesota	$16,002	$16,002	
Johnson County, Warrensburg, Missouri	$19,446	$19,446	
Kickapoo Tribe of Oklahoma, McLoud, Oklahoma	$79,770	$79,770	
Miami/Miami-Dade Weed and Seed, Inc., Miami, Florida	$124,141		
Minnesota Program Development, Inc., Duluth, Minnesota	$114,039	$114,039	
Montgomery County, Independence, Kansas	$69,400	$69,400	
OJP Grants Awarded to the Washington Department of Corrections, Olympia, Washington	$679,234	$679,234	
OJP Southwest Border Prosecution Initiative Funding, City and County of San Francisco, California	$5,414,895		

Quantifiable Potential Monetary Benefits

Audit Report	Questioned Costs	Unsupported Costs	Funds Put to Better Use
OJP Southwest Border Prosecution Initiative Funding Received by Brooks County, Texas	$1,921,274	$793,365	
OJP BJA Community Justice Empowerment Project Grant Administered by the National Training and Information Center, Chicago, Illinois	$3,067,800	$97,063	$94,780
OJP BJA Grant Awarded to the 7th Judicial Administrative District, State of Georgia for the Tallapoosa Drug Intervention Program, Cartersville, Georgia	$1,291	$1,291	
OJP BJA Grant Awarded to the City and County of Denver, Colorado	$153,327		$80,027
OJP BJA Tribal Drug Courts Grant to the Crow Tribe of Indians Crow Agency, Montana	$65,107	$65,107	
OJP NIJ Cooperative Agreement Awarded to the North Dakota State University	$5,116	$978	
OJP Office of Juvenile Justice and Delinquency Prevention Grant Administered by the Boys and Girls Home Residential Treatment Center, Inc., Sioux City, Iowa	$65,920	$65,920	
OJP OVC Grants Administered by the Illinois Court of Claims, Springfield, Illinois	$447,194	$447,194	
OJP OVC Services for Trafficking Victims Discretionary Grant Program, Cooperative Agreement Awarded to the International Rescue Committee, New York, New York	$487,702	$487,702	
OJP Office of Violence Against Women Legal Assistance for Victims Grant and Services for Human Trafficking Victims Grants Administered by the Heartland Alliance for Human Needs and Human Rights	$1,675,412	$1,367,753	
St. Louis County, St. Louis, Missouri	$6,430		
State of Connecticut, Hartford, Connecticut	$281	$281	

Quantifiable Potential Monetary Benefits

Audit Report	Questioned Costs	Unsupported Costs	Funds Put to Better Use
State of Louisiana, Baton Rouge, Louisiana	$126,251		
State of Nebraska, Lincoln, Nebraska	$414,147	$414,147	
State of North Dakota, Bismarck, North Dakota	$2,074	$2,074	
State of South Carolina, Columbia, South Carolina	$462,191	$404,639	
State of Washington, Olympia, Washington	$652,646	$652,646	
Tangipahoa Parish Sheriff, Amite, Louisiana	$33,043	$33,043	
The Navaho Nation, Window Rock, Arizona	$4,087,748	$4,087,748	
Town of Brattleboro, Vermont	$2,054	$2,054	
University of Missouri, Columbia, Missouri	$130,608	$130,608	
University of Notre Dame, Notre Dame, Indiana	$6,670	$6,670	
University of Toledo, Toledo, Ohio	$1,200	$1,200	
Use of Equitable Sharing Revenues by the Douglas County Sheriff's Office, Omaha, Nebraska	$4,750		
Total	***$20,865,895***	***$10,355,920***	***$174,807***

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	41
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	7-40
Section 5(a)(2)	Significant Recommendations for Corrective Actions	7-39
Section 5(a)(3)	Prior Significant Recommendations Unimplemented	44-45
Section 5(a)(4)	Matters Referred to Prosecutive Authorities	12, 19-21, 24-26, 31-32, 35, 38
Section 5(a)(5)	Refusal to Provide Information	None
Section 5(a)(6)	Listing of Audit Reports	49-55
Section 5(a)(7)	Summary of Significant Reports	7-39
Section 5(a)(8)	Audit Reports – Questioned Costs	43
Section 5(a)(9)	Audit Reports – Funds to Be Put to Better Use	42
Section 5(a)(10)	Prior Audit Reports Unresolved	44
Section 5(a)(11)	Significant Revised Management Decisions	None
Section 5(a)(12)	Significant Management Decisions with which the OIG Disagreed	None

Report Waste, Fraud, Abuse, or Misconduct

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

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

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

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

Report Violations of Civil Rights and Civil Liberties

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

Civil Rights and Civil Liberties Complaints
Office of the Inspector General

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

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

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