Office of the Inspector General Semiannual Report to Congress

April 1, 2006 – September 30, 2006

Message From the Inspector General

This semiannual period was marked by the death of Office of the Inspector General (OIG) Special Agent William "Buddy" Sentner III, who was shot and killed in the line of duty on June 21, 2006. Agent Sentner was working as part of a team to execute arrest warrants on six federal correctional officers in Tallahassee, Florida. The six correctional officers were charged with conspiring to sexually abuse female inmates and to introduce contraband into the prison. During the execution of the arrest warrants, one of the correctional officers who was being arrested opened fire on the arrest team. Acting with extraordinary courage, Agent Sentner engaged the officer and returned fire, killing the correctional officer. Agent Sentner was killed and a Federal Bureau of Prisons (BOP) employee was wounded by the correctional officer. Agent Sentner's brave actions under fire saved the lives of several other federal employees while sacrificing his own life.

Like other OIG agents, Agent Sentner recognized that his job was dangerous and difficult. It is not easy to investigate federal employees who abuse their trust and prey upon others. But Agent Sentner did not shy away from duty or danger. He, and other OIG agents, worked tirelessly to make the Department of Justice, and the country, better and safer. In my view, Buddy Sentner lived like a hero and died like a hero.

This semiannual report contains a tribute to Buddy Sentner. His courage also was recognized by the 2006 Attorney General's Award for Exceptional Heroism, which was bestowed on him posthumously. In addition, the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency, a group of Inspectors General from throughout the federal government, created an award in Buddy's name to honor OIG employees who exhibit exceptional dedication to duty.

In this semiannual report, we also summarize other OIG investigations, inspections, audits, and special reviews. As described throughout this report, OIG investigators continued their important work investigating allegations of criminal and administrative misconduct by Department of Justice (Department) employees and contractors.

Our audits, evaluations, and special reviews have continued to concentrate on the Department's top management and performance challenges, including counterterrorism, efforts to upgrade the Department's information technology (IT) systems, and attempts to improve the sharing of intelligence and law enforcement information. For example, during this reporting period we examined the Federal Bureau of Investigation's (FBI) progress toward achieving interoperability between its fingerprint system and the Department of Homeland Security's (DHS) fingerprint system; the BOP's efforts to prevent terrorists and other high-risk inmates from using the mail to encourage terrorists or criminal activities; and the FBI's performance in connection with the handling of Katrina Leung, an asset in its Chinese counterintelligence program who had a long-term intimate relationship with her FBI handler.

We also completed other significant reviews this reporting period, such as our follow-up review assessing the Drug Enforcement Administration's (DEA) actions to control the illegal diversion of prescription drugs and a report examining the shooting incident involving the FBI and Filiberto Ojeda Ríos, a federal fugitive and leader of a Puerto Rican pro-independence organization.

We appreciate the support that we have received from both the Department and the Congress as we conduct our important oversight work. Finally, I want to express our gratitude for the outpouring of support from the Department, the OIG community, other law enforcement agencies, and many individuals to the OIG and Buddy Sentner's family in response to his death. He made the ultimate sacrifice in the line of duty, and we will always be inspired by his example as we carry on with the important work of the OIG.

Glenn A. Fine
Inspector General
October 31, 2006

Table of Contents

Highlights of OIG Activities 1
OIG Profile 5
Federal Bureau of Investigation 7
Federal Bureau of Prisons 18
Bureau of Alcohol, Tobacco, Firearms and Explosives 23
U.S. Marshals Service 26
Drug Enforcement Administration 28
Office of Justice Programs 30
Other Department Components 32
- U.S. Attorneys' Offices 32
- Civil Rights Division 33
- Criminal Division 33

Multicomponent Audits, Reviews, and Investigations 35
Top Management and Performance Challenges 41
Congressional Testimony 42
Legislation and Regulations 42
Statistical Information 43
- *Audit Statistics* 43
- Funds Recommended for Better Use 43
- Questioned Costs 44
- Management Improvements 44
- Audit Follow-Up 45
- Unresolved Audits 45
- *Evaluation and Inspections Statistics* 46
- *Investigations Statistics* 46

Appendices
- Acronyms and Abbreviations 47
- Glossary of Terms 48
- Evaluation and Inspections Division Reports 49
- Audit Division Reports 50
- Reporting Requirements Index 55

Highlights of OIG Activities

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

Statistical Highlights

April 1, 2006 — September 30, 2006

Allegations Received by the Investigations Division	4,724
Investigations Opened	193
Investigations Closed	202
Arrests	86
Indictments/Informations	83
Convictions/Pleas	61
Administrative Actions	89
Fines/Restitutions/Recoveries	$136,986
Audit Reports Issued	105
Questioned Costs	$10 million
Funds Put to Better Use	$3 million
Recommendations for Management Improvements	335

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

- **The BOP's Monitoring of Mail for High-Risk Inmates.** The OIG evaluated the BOP's efforts to prevent terrorists and other high-risk inmates from using the mail or the cover of a foreign language to continue or encourage criminal or terrorist activities. We found that the BOP does not adequately read the mail or listen to the telephone calls, visitor communications, or cellblock conversations of terrorists and high-risk inmates; does not have sufficient resources to translate inmate communications in foreign languages; and lacks staff that is adequately trained in intelligence analyses techniques to properly assess terrorism communications. We made 15 recommendations to assist the BOP in improving its monitoring of mail and verbal communications of terrorists and high-risk inmates.

- **Review of the FBI's Handling of Intelligence Information Related to the September 11 Attacks.** The OIG released an unclassified version of its full report on the "FBI's Handling of Intelligence Information Prior to the September 11 Attacks." This report includes a previously unreleased chapter on the FBI's investigation of Zacarias Moussaoui, a French citizen who is serving a life sentence after pleading guilty to charges related to his participation in a plot to fly planes into buildings. The OIG could not previously release the portions of the unclassified report related to Moussaoui because his trial was pending. This chapter of the report analyzes the efforts by the Minneapolis FBI in August 2001 to obtain a warrant to search Moussaoui's computer and belongings after his arrest. We found significant problems with the FBI's handling of the Moussaoui case that were attributable to both systemic issues — how it handled intelligence and counterterrorism issues at the time — and

failings on the part of individuals involved in the case.

- **Review of the FBI's Attempt to Arrest Filiberto Ojeda Ríos.** At the request of the FBI Director, the OIG reviewed the shooting incident involving the FBI and Filiberto Ojeda Ríos, a fugitive who was the leader of a clandestine Puerto Rican pro-independence organization. During an attempted capture of Ojeda at his residence in western Puerto Rico, the FBI and Ojeda engaged in a brief but intense exchange of gunfire that resulted in Ojeda striking and seriously injuring an FBI agent. The exchange was followed by a standoff during which FBI agents unsuccessfully tried to persuade Ojeda to surrender. Later, an FBI agent saw Ojeda in the window with a gun in his hand and fired three shots, one of which struck Ojeda. Although several agents heard Ojeda cry out and fall, the FBI did not enter the house until the next day, at which time FBI agents found Ojeda dead on the floor. We concluded that the FBI agents' use of force in the Ojeda operation did not violate the Department's Deadly Force Policy. We also determined that the FBI's cautious approach toward entering the residence after Ojeda was shot was motivated by considerations of agent safety, not by any desire to withhold medical treatment from Ojeda. However, we cited several deficiencies in the planning and execution of the attempted arrest and made 10 recommendations to improve future FBI arrest operations.

- **Review of the FBI's Handling and Oversight of Asset Katrina Leung.** The OIG examined the FBI's handling and oversight of Katrina Leung, one of the FBI's highest paid counterintelligence assets who allegedly also worked for the People's Republic of China. Leung had a longtime intimate relationship with her FBI handler, Special Agent James J. Smith. We found that the FBI was aware of serious counterintelligence concerns about Leung, but did little to follow up on the warning signals it received. Since this mishandling came to light, the FBI has taken steps to correct deficiencies in its China Program and improve asset handling and vetting procedures. We provided 11 recommendations to help further address the systemic issues that enabled Smith and Leung to escape detection for more than 20 years.

- **Follow-Up Review of the FBI's Progress Toward Biometric Interoperability between Fingerprint Systems.** This OIG evaluation reported on the progress of the FBI and the DHS toward achieving biometric interoperability between the FBI's Integrated Automated Fingerprint Identification System and the DHS's Automated Biometric Identification System. The two agencies have resolved a major impasse and are now implementing the first phase of a three-phase plan to make the fingerprint systems fully interoperable by December 2009. Fully interoperable fingerprint systems will allow law enforcement and immigration officers to more readily identify criminals and known or suspected terrorists trying to enter the United States and those already in the country.

- **Review of ATF's Violent Crime Impact Team Initiative.** An OIG review of the Bureau of Alcohol, Tobacco, Firearms and Explosives' (ATF) Violent Crime Impact Team (VCIT) initiative concluded that, while the initiative may be an effective tool to reduce violent crime in targeted areas, inconsistent oversight and direction from ATF have allowed local VCITs to ignore key elements of the strategy. We also found that ATF's claim that it had met its stated goals was based on insufficient data. We made five recommendations to improve ATF's implementation of the VCIT initiative, including establishing specific operational guidelines for VCIT implementation and

developing an adequate evaluation strategy to assess the success of the VCIT program.

- **Follow-Up Review of the DEA's Efforts to Control the Diversion of Controlled Pharmaceuticals.** The OIG conducted a follow-up review on the DEA's actions to control the illegal diversion of pharmaceutical drugs. We found that the DEA has taken important steps to improve its ability to control the diversion of pharmaceuticals, especially over the Internet. Those steps include centralizing diversion criminal investigations with other criminal investigations and providing additional intelligence resources to diversion investigators. Despite these positive actions, we also found several shortcomings that were first reported in our 2002 review. Specifically, the time spent by special agents assisting diversion investigations still constitutes a small share of their total investigative effort, the diversion groups in the field receive only limited support from intelligence analysts, and intelligence analysts and special agents are offered minimal diversion control training. We made six recommendations to help the DEA further improve its ability to address the growing problem of diversion of controlled pharmaceuticals.

Investigations

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

- A joint investigation by the OIG and the FBI led to the indictment of six BOP correctional officers assigned to the Federal Correctional Institution in Tallahassee, Florida, on charges of conspiracy to sexually abuse female inmates and introduction of contraband. OIG investigators developed evidence that the correctional officers were involved in a scheme to provide contraband to female inmates in exchange for sexual favors and money. Two of the correctional officers pled guilty and are awaiting sentencing, and three correctional officers are involved in judicial proceedings. The sixth correctional officer and OIG special agent William "Buddy" Sentner III were killed in an exchange of gunfire initiated by the correctional officer during the execution of the arrest warrants.

- An OIG investigation led to the arrest of a painter who received more than $1 million from the September 11 Victim Compensation Fund based on his fraudulent claim that he was permanently disabled and unable to work as a result of back injuries sustained during the September 11 terrorism attacks. Videotape evidence gathered by the OIG demonstrated that the painter continued to engage in physical activities, such as bicycling and dancing, which were inconsistent with the injuries he claimed. In addition, the OIG gathered evidence that the painter continued to paint houses in his neighborhood and that he fraudulently concealed pre-existing injuries from the hearing officer who evaluated his disability claim.

- A former special agent in charge (SAC) of the FBI's El Paso field office was convicted of making false statements. The jury found that the SAC concealed material facts from the FBI concerning his relationship and financial dealings with a Mexican national who had alleged Mexico drug cartel associations and was a former confidential informant. The jury also found that the SAC made false statements when he failed to disclose in his 2002 financial disclosure report that the former confidential

informant provided the SAC with paid family vacations to Las Vegas and Mexico, an El Paso country club membership, weekly residential lawn service, and a $5,000-per-month job for the SAC's wife. In return, the SAC assisted the former confidential informant by attempting to resolve his numerous visa issues.

- A former FBI telecommunications specialist pled guilty to charges of embezzlement and theft of public money, property, or records after OIG investigators found that the specialist stole $27,000 from telephone company refund checks intended for the FBI.

- Two BOP correctional officers are being prosecuted on charges of deprivation of civil rights under color of law, conspiracy, aiding and abetting, and obstruction of justice after OIG investigators developed evidence that the correctional officers beat an inmate in his cell, blocked the views of surveillance cameras to conceal the incident, and made false entries in government documents.

- An OIG investigation of an Office of Justice Programs (OJP) contracting specialist who accepted gratuities from a contractor led to the specialist receiving a 45-day suspension, reassignment to a non-procurement position, and permanent revocation of her contracting warrant.

Ongoing Work

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

- Coordination of Violent Crime Task Forces in the Department

- Review of Cost Tracking and Planning for the Department's IT Initiatives

- The Department's Internal Controls Over Terrorism Reporting Statistics

- The FBI's Use of Certain *USA PATRIOT Act* (Patriot Act) Authorities

- Review of the FBI's Sentinel IT Project

- Follow-Up Review of the FBI's Response to Recommendations Made in the Robert Hanssen Review

- Follow-Up Review of the FBI's Control Over Weapons and Laptop Computers

- The U.S. Marshals Service's (USMS) Justice Prisoner and Alien Transportation System

- DEA Controls Over Cash Seizures

OIG Profile

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

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

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

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

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

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

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

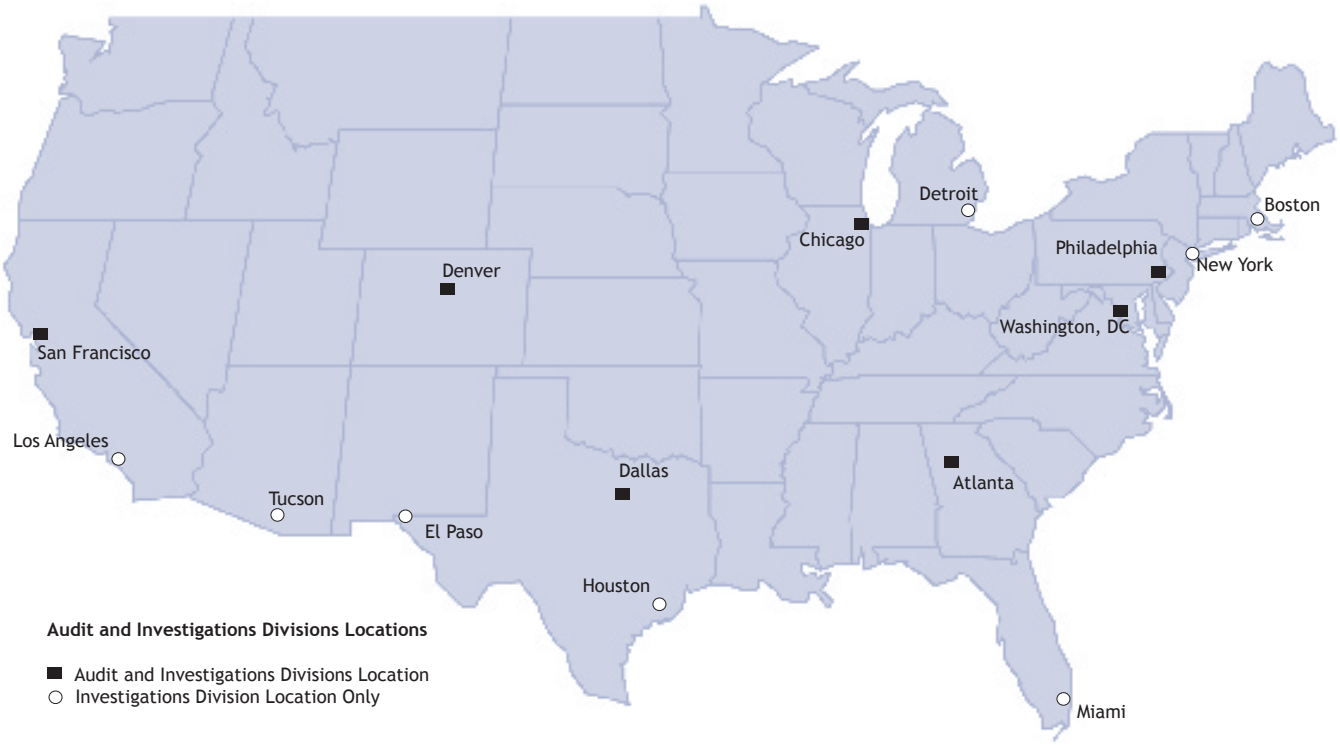
components in the areas of budget formulation and execution, security, personnel, training, travel, procurement, property management, information technology, computer network communications, telecommunications, quality assurance, internal controls, and general support.

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

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

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

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



Federal Bureau of Investigation

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

Reports Issued

Review of the FBI's Handling of Intelligence Information Related to the September 11 Attacks

In June 2006, the OIG's Oversight and Review Division released an unclassified version of the full report it completed in 2004 entitled, "A Review of the FBI's Handling of Intelligence Information Prior to the September 11 Attacks." The June 2006 version contains a chapter that was previously unreleased to the public concerning the FBI's investigation of Zacarias Moussaoui. The OIG could not previously release portions of the unclassified report related to Moussaoui because his trial was pending at the time.

The report describes the FBI's investigation of Moussaoui, who was arrested on immigration charges in Minneapolis on August 16, 2001. After Moussaoui's arrest, the Minneapolis FBI, concerned that Moussaoui was training to possibly commit a terrorist act involving a commercial airplane, attempted to investigate his potential links to terrorism by seeking a warrant to search Moussaoui's computer and other belongings. However, FBI Headquarters did not believe that a sufficient predicate existed to obtain either a criminal warrant or a *Foreign Intelligence Surveillance Act* (FISA) warrant. At the time of the September 11 attacks, Moussaoui remained in custody, and the FBI planned to deport him to France.

The OIG found significant problems with the FBI's handling of the Moussaoui case that were attributable to both systemic issues — how it handled intelligence and counterterrorism issues at the time — and failings on the part of some of the individuals involved in the case. We concluded, however, that no FBI employee committed intentional misconduct or attempted to deliberately sabotage the Minneapolis FBI's request for a FISA warrant, as one FBI employee charged. We did find that the Minneapolis FBI agents, who deserved credit for their tenacity and accurate instincts, did not receive sufficient support either from their field office management and legal counsel or FBI Headquarters.

The Moussaoui case illustrated systemic problems with the FBI's handling of intelligence cases at the time, including a narrow and conservative interpretation of the FISA requirements, inadequate analysis of whether to proceed as a criminal or intelligence investigation, adversarial relations between FBI Headquarters and the field, and inadequate and disjointed reviews of potential FISA requests by FBI attorneys. While some of the information contained in this report was released during the Moussaoui trial, the report provides additional details as well as a step-by-step chronology of the FBI's handling of the Moussaoui investigation both in the field and at FBI Headquarters.

Our full report found significant deficiencies in the FBI's handling of intelligence information related to September 11, and concluded that the FBI failed to fully evaluate, investigate, exploit, and disseminate the information it had received about: 1) efforts by Usama Bin Laden to send students to attend United States civil aviation schools to conduct terrorist activities and 2) two of the September 11 hijackers — Nawaf al Hazmi and Khalid al Mihdhar. In the final report, the OIG made 16 recommendations for improving the FBI's intelligence and counterterrorism efforts.

In response to the report, the FBI said it has upgraded the physical infrastructure in FBI field offices to handle classified information, established centralized intelligence components in each field office, and trained employees on subjects such as disseminating threat-related information and FISA.

Review of the FBI's Attempt to Arrest Filiberto Ojeda Ríos

In August 2006, the OIG's Oversight and Review Division issued its report on the shooting incident involving the FBI and long-time fugitive Filiberto Ojeda Ríos — the leader of a clandestine Puerto Rican pro-independence organization that claimed credit for violent crimes during the 1970s and 1980s. On September 23, 2005, FBI agents approached a residence in western Puerto Rico to arrest Ojeda. The operation resulted in a brief but intense exchange of gunfire between Ojeda and the FBI in which one FBI agent was seriously wounded. The exchange was followed by a standoff during which FBI agents unsuccessfully tried to persuade Ojeda to surrender. Later, an FBI agent observed Ojeda with a gun in his hand and fired three shots, one of which struck Ojeda. Although several agents heard Ojeda cry out and fall, no one entered the house until the next day, at which time FBI agents found Ojeda dead on the floor.

Several journalists, elected officials, and activists in Puerto Rico criticized the FBI for using excessive force to capture Ojeda and for waiting 18 hours after Ojeda was shot before entering his residence. As a result, the FBI Director requested that the OIG review the circumstances surrounding the FBI's arrest operation and the death of Ojeda.

We concluded that the FBI agents' use of force in the Ojeda operation did not violate the Department's Deadly Force Policy, which states that Department law enforcement officers may use deadly force when the officer "has a reasonable belief that the subject of such force poses an imminent danger of death or serious physical injury to the officer or to another person." The OIG found that Ojeda became aware that the FBI was coming to arrest him, made preparations to resist arrest, and opened fire on the agents as they attempted to enter the residence and before any agents had discharged their weapons. The OIG concluded that once Ojeda began firing he posed an imminent danger to the agents, and the agents were justified in returning fire.

We also determined that the FBI's cautious approach toward entering the residence after

Ojeda was shot was motivated by considerations of agent safety, not by any desire to withhold medical treatment from Ojeda. The FBI's concern during this period was that Ojeda might not be incapacitated and there might be a second gunman inside the house because the arrest team believed that more than one weapon had been fired at them during the initial gunfight. FBI Headquarters officials also were concerned that it would be difficult to detect improvised explosive devices inside the house at night. Moreover, the OIG found that the decision to delay entry until the next day likely had no impact on Ojeda's death. The forensic pathologist from the Puerto Rico Institute of Forensic Sciences who performed the autopsy estimated that Ojeda died from blood loss approximately 15 to 30 minutes after being shot.

However, the OIG report cited deficiencies in several aspects of the FBI's planning and execution of the attempted arrest. For example, we determined that the decision to conduct an emergency daylight assault to arrest Ojeda was extremely dangerous and not the best option available. Moreover, the FBI had sufficient information to expect that Ojeda would be prepared to resist an arrest attempt with violence, as he had done in the past, and that he would have a significant advantage over the arresting agents in terms of cover, elevation, and visibility. Conversely, a strategy of surrounding the residence and calling for Ojeda to surrender, with the option of using chemical agents such as tear gas to force Ojeda outside, would have been a safer and potentially more effective strategy.

Our report provided 10 systemic recommendations to improve the planning and conduct of future FBI arrest operations, including ensuring the reconsideration of all relevant tactical options when circumstances change and ensuring that negotiations are integrated into tactical planning for operations in which a standoff is a foreseeable contingency.

Review of the FBI's Handling and Oversight of Asset Katrina Leung

In May 2006, the OIG's Oversight and Review Division issued a classified report and unclassified executive summary examining the FBI's handling and oversight of Katrina Leung, one of its highest paid counterintelligence assets. Leung and her FBI handler of 18 years, Special Agent James J. Smith, were arrested in April 2003 after an FBI investigation alleged that Leung had been spying for the People's Republic of China against the United States. The FBI investigation also found that Leung and Smith had been involved in an intimate romantic relationship for nearly 20 years. Following the arrests of Smith and Leung, the FBI Director asked the OIG to review the performance and management issues related to this case.

We found that Smith operated Leung with little oversight based primarily on his status as a top agent in Los Angeles and Leung's status as a highly valued asset. We also determined that the FBI was aware of serious counterintelligence concerns about Leung that began to surface during the late 1980s and early 1990s, but did little to follow up on the warning signals it received. Consequently, the FBI's inattention to the oversight of Smith and Leung, its willingness to exempt Smith from complying with the rules governing asset handling, and its failure to aggressively question Smith or follow up when red flags arose allowed Leung to deceive the FBI about the extent of her spying for the People's Republic of China and permitted Smith to continue his affair with Leung until his retirement in November 2000.

In May 2000, the FBI received credible information indicating that Leung was a spy for the People's Republic of China and that she had a source in the FBI's Los Angeles Division. The FBI inappropriately informed Smith about this

information — which implicated him — and did not begin an investigation of Smith and Leung until a year later. The OIG concluded that in light of the serious nature and specificity of the allegation, there was no reasonable explanation for the FBI's delay in opening the investigation.

Since the discovery of Smith's long-term relationship with Leung, the FBI has taken steps to correct deficiencies in its China Program and improve asset handling and vetting procedures. However, the OIG report also provided 11 recommendations to help further address the systemic issues that enabled Smith and Leung to escape detection and avoid accountability. The recommendations included requiring separate documentation for red flags and other counterintelligence concerns involving assets, requiring alternate case agents to frequently meet with assets, limiting the time a single agent can handle an asset, and fully implementing the FBI's policy regarding counterintelligence polygraph examinations.

The FBI's Investigative Activities Concerning Potential Protesters at the 2004 Democratic and Republican National Political Conventions

In 2004, news articles reported that the FBI questioned political demonstrators across the United States in connection with threatened violent and disruptive protests at the Republican and Democratic National Conventions held that summer. The articles stated that dozens of people had been interviewed in at least six states, including anti-war demonstrators and political demonstrators and their friends and family members. Following publication of the news articles, several members of Congress requested that the OIG initiate an investigation into "possible violations of First Amendment free speech and assembly rights by the Justice Department in connection with their investigations of possible protests at the Democratic and Republican political conventions in Boston and New York and other venues."

In April 2006, the OIG's Oversight and Review Division issued its report on the FBI's use of its investigative authorities to conduct interviews of potential protesters in advance of the 2004 national political conventions. The OIG review did not substantiate allegations that the FBI improperly targeted protesters for interviews in an effort to chill the exercise of their First Amendment rights at the 2004 national political conventions. The OIG concluded that FBI interviews of potential convention protesters and other related interviews, together with its related investigative activities, were conducted for legitimate law enforcement purposes based on information associated with possible bomb threats and other violent criminal activities.

The OIG found that nearly all of the protester-related investigative activity was devoted to addressing 17 distinct threats to the conventions falling within the FBI's domestic terrorism program. The report concluded that the FBI addressed each threat in accordance with the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (General Crimes Guidelines). In addition, the review identified seven terrorism enterprise investigations not initiated in connection with the conventions that generated convention-related criminal intelligence. The OIG concluded that the investigative techniques used to obtain this intelligence were a logical outgrowth of the underlying investigations, and that the investigative activity was undertaken in a manner consistent with the requirements of the General Crimes Guidelines.

Follow-Up Review of the FBI's Progress Toward Biometric Interoperability Between Fingerprint Systems

The OIG's Evaluation and Inspections Division continued its monitoring of the FBI's progress toward achieving biometric interoperability between its Integrated Automated Fingerprint Identification System (IAFIS) and the DHS's Automated Biometric Identification System (IDENT). Our latest of six reports described how the FBI and the DHS have resolved a major impasse and are now implementing the first phase of a three-phase plan to make the fingerprint systems fully interoperable by December 2009.

In our previous reports, we described how fully interoperable fingerprint systems would allow law enforcement and immigration officers to more readily identify criminals and known or suspected terrorists trying to enter the United States and those already in the country. However, the FBI and the former Immigration and Naturalization Service (INS), now part of the DHS, developed separate automated fingerprint systems in the early 1990s — IAFIS is based on 10 rolled fingerprints while IDENT uses 2 flat fingerprints. In our December 2004 report, we found that the differing fingerprint collection requirements and preferences had created an impasse that stalled interoperability efforts. Our latest report related that this impasse was resolved when the DHS agreed to modernize IDENT and convert US-VISIT — its entry/exit and border security system — from a 2- to a 10-fingerprint system.

In addition, the FBI and the DHS agreed to a three-phase plan that will make their systems fully interoperable by December 2009. In the first phase, the FBI and the DHS will deploy a joint automated system for sharing key immigration and law enforcement data. In the latter two phases, the agencies will expand the amount of immigration and law enforcement data shared and allow access to that data by federal, state, and local law enforcement agencies. When the interoperability effort is completed, a single request will search all fingerprint records maintained by the FBI and the DHS, and the requestor will receive all associated criminal history and immigration information about an individual.

While the FBI and the DHS continue their efforts to employ a fully interoperable system by 2009, the FBI has taken interim steps to reduce the risk that criminal aliens or terrorists will enter the United States undetected. As we recommended in our December 2004 report, the FBI has increased the transmission of "Known or Suspected Terrorists" records to the DHS from monthly to daily. In addition, the FBI has improved the overall availability of IAFIS to all users, has increased its capacity for DHS-requested fingerprint searches, and has reduced the response time to DHS requests for checks of aliens' fingerprints. However, until full IDENT/IAFIS interoperability is achieved, the DHS's policy of using IAFIS to check the fingerprints of less than 1 percent of the visitors subjected to US-VISIT will continue the risk that criminal aliens or terrorists could enter the United States undetected.

Combined DNA Index System Operational and Laboratory Vulnerabilities

The OIG's Audit Division examined the FBI's Combined DNA Index System (CODIS), a national DNA-profile matching service that contains DNA profiles from crime scenes, convicted offenders, and sources involving missing

persons. CODIS enables federal, state, and local crime laboratories to electronically compare over 3.1 million DNA profiles for crime solving and identifying missing or unidentified persons. The FBI CODIS Unit is responsible for overseeing CODIS operations and ensuring that these activities are conducted appropriately.

Our report followed up on an OIG audit conducted in 2001 that recommended the FBI improve its oversight of CODIS–participating laboratories to ensure compliance with applicable standards. In our latest report, we found that the FBI has improved several aspects of CODIS operations, but must make further progress to ensure that it properly oversees the CODIS program and its participants. Through a comprehensive national survey of laboratories participating in CODIS, we found that the FBI received an overall positive evaluation regarding its administration of CODIS. However, we also found that the FBI could improve the CODIS community's understanding and compliance with applicable standards by providing key CODIS laboratory staff with training on quality assurance standards, by tracking findings identified in quality assurance audits of state and local CODIS laboratories, and by placing a greater emphasis on written rather than verbal guidance to the CODIS community.

In addition, we found that the FBI has not implemented routine audits of forensic profiles uploaded into CODIS, instead relying on participating laboratories to annually certify that they are in compliance with CODIS standards. For example, in 18 OIG audits of participating laboratories during FYs 2004 and 2005, we found 13 incidents where forensic profiles uploaded in CODIS violated some aspect of CODIS requirements. In four of those instances, profiles matching the victim of the crime were inappropriately uploaded into CODIS, and in two instances profiles matching a known person who was not a suspected perpetrator were inappropriately uploaded into CODIS. Six of the 18 laboratories audited had not obtained the certification forms from laboratory employees stating that they agreed to upload only allowable profiles into the CODIS database.

We concluded that these weaknesses leave CODIS potentially vulnerable to undetected, inadvertent, or willful non-compliance by CODIS participants and consequently could undermine the integrity of the CODIS program. We made 22 recommendations to the FBI to better protect the integrity of CODIS data by implementing additional internal controls over data compliance, tracking audit findings, and conducting routine audits of forensic profiles to verify compliance. The FBI agreed with 19 of the 22 recommendations.

CODIS Audits of State and Local Laboratories

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

- The Tennessee Bureau of Investigation Forensic Services Division's Nashville Laboratory in Nashville, Tennessee, was in compliance with standards governing CODIS activities for the areas tested with five exceptions: 1) the Nashville Laboratory had given an individual access to CODIS without proper authorization, 2) the Nashville Laboratory's last external evaluation report

was not forwarded to the NDIS Custodian within the required 30 days, 3) the Nashville Laboratory uploaded 14 unallowable forensic profiles into CODIS, 4) two specimen identification numbers had to be corrected, and 5) one convicted offender profile had to be corrected in CODIS to include a second value for one of the loci tested. We recommended that the FBI ensure that the Nashville Laboratory establish a procedure to submit appropriate paperwork before providing its personnel with CODIS access, ensure that the Nashville Laboratory establish a procedure to forward external laboratory evaluations to the NDIS Custodian within 30 days of receipt or request an extension of time, and require that the Nashville Laboratory conduct a review of all forensic profiles to ensure that there are no other unallowable profiles in NDIS and all specimen identification numbers are complete and accurate. The FBI agreed with the recommendations and has begun implementing corrective measures.

- The Massachusetts State Police Crime Laboratory in Sudbury, Massachusetts, was not in compliance with all the standards governing CODIS activities for the areas we tested. The Massachusetts Laboratory was not in compliance with the NDIS requirements because: 1) one case file did not contain documentation indicating that the Massachusetts Laboratory had confirmed or refuted a potential match, 2) a second match was not confirmed until almost 8 months after the Massachusetts Laboratory was notified of the potential match, and 3) the external evaluation report was sent to the NDIS Custodian almost 7 months late. In addition, our tests of 100 forensic profiles the Massachusetts Laboratory had uploaded to the national database disclosed that 14 profiles were incomplete, 2 profiles were inaccurate, and 1 profile was both incomplete and inaccurate. We recommended that the FBI require the Massachusetts Laboratory to implement internal control procedures to: 1) ensure it resolves all candidate matches within 30 business days and document the resolutions to meet the NDIS participation requirements, 2) ensure it forwards all external audit evaluations to the NDIS Custodian within the timeframe required by the NDIS participation requirements, and 3) ensure all DNA profiles uploaded to NDIS are complete, accurate, and allowable. The FBI responded that it would obtain additional information from the Massachusetts Laboratory to ensure that it complies with NDIS standards.

The FBI's Implementation of the Laboratory Information Management System

The FBI Laboratory in Quantico, Virginia, is one of the largest and most comprehensive forensic laboratories in the world, conducting over 1 million examinations of physical evidence annually. However, the FBI Laboratory relies on an outdated system to manage the evidence that passes through the Laboratory. The current system is a database that shows when an item enters the Laboratory for testing, when analyses are performed, and when the item leaves the Laboratory. It does not, however, readily locate evidence within the Laboratory, determine what work remains to be completed, or provide reports to help manage Laboratory operations.

To remedy the limitations of the existing system, the FBI contracted with a private company in September 2003 to provide the FBI with a commercial-off-the-shelf Laboratory Information Management System (LIMS), which would be used to track evidence using bar-code technology and provide a variety of other reporting capabilities. We had recommended in a 2004

review of protocol and practice vulnerabilities in the FBI DNA Laboratory that the FBI's plans to implement the LIMS by the end of FY 2004 should remain a top priority because the system would reduce the incidents of error and allow staff members to be more efficient in performing their duties. However, our current report found that after many delays and extensive customization of LIMS, the system was unable to meet the FBI's security requirements. In March 2006, the FBI and the private company agreed to terminate the LIMS contract, resulting in an overall loss to the FBI of $1.18 million.

The OIG's Audit Division determined that because the LIMS project began before the FBI established its Information Technology Investment Management processes, the FBI did not have the capability early on to identify problems with the contract. Additionally, the FBI did not adequately document the security requirements for certification and accreditation of the LIMS software and, to the extent security requirements evolved, did not clarify those changes through contract modifications.

With the termination of the LIMS project, the FBI's Laboratory Division still lacks a modern system to track evidence and otherwise effectively manage its Laboratory operations. The OIG made three recommendations to the FBI, including ensuring that any future Laboratory information management system is overseen by an experienced IT project manager. The FBI agreed with all the recommendations.

Investigations

During this reporting period, the OIG received 689 complaints involving the FBI. The most common allegations made against FBI employees were Intelligence Oversight Board violations, job performance failure, waste or misuse of government property, and misuse of a credit card. The OIG opened 12 cases and referred 660 allegations to the FBI's Inspection Division.

At the close of the reporting period, the OIG had 39 open cases of alleged misconduct against FBI employees. The criminal investigations cover a wide range of offenses, including fraud, release of information, and theft. The administrative investigations include serious allegations of misconduct, such as allegations against high-level employees. The following are examples of cases involving the FBI that the OIG's Investigations Division investigated during this reporting period:

- An investigation by the OIG's Dallas Field Office led to the conviction in the Western District of Texas of a former FBI special agent in charge (SAC) on charges of making false statements. The jury found that the SAC concealed material facts from the FBI concerning his relationship and financial dealings with a Mexican national who had alleged Mexico drug cartel associations and was a former confidential informant. The SAC also made false statements on his 2002 Public Financial Disclosure Report regarding gifts he received from the former confidential informant.

  The OIG investigation found that the SAC, after being directed by the FBI to fully disclose his relationship with the former confidential informant, failed to disclose that the former confidential informant paid for the SAC's family vacations to Las Vegas and Mexico, an El Paso country club membership, weekly residential lawn service, and a $5,000-per-month job for the SAC's wife. In return, the SAC assisted the former confidential informant by attempting to resolve his numerous visa issues. In addition, the SAC met with and provided assurance to potential American

investors who were interested in the former confidential informant's racetrack. Further, the SAC held a press conference in Mexico and vouched for the former informant. The SAC, a 23-year veteran of the FBI, retired 2 days after his OIG interview. Sentencing is pending.

- An investigation by the OIG's Houston Area Office led to the arrest and guilty plea of a former FBI telecommunications specialist assigned to the Houston Field Division on charges of embezzlement and theft of public money, property, or records. OIG investigators developed evidence that the telecommunications specialist stole $27,000 from telephone company checks intended for the FBI as refunds for overpayment for covert telephone services. The FBI employee resigned from her position as a result of this investigation. Sentencing is pending.

- A joint investigation by the OIG's San Francisco Area Office and the FBI led to the arrest of an FBI accounting technician assigned to the Honolulu Division on charges that the accounting technician and 7 co-defendants conspired to distribute 50 grams or more of methamphetamine. The accounting technician also confessed to OIG investigators that she inappropriately obtained and disseminated information from the FBI's computer database related to an ongoing drug investigation involving her relatives. The FBI placed the accounting technician on unpaid administrative leave. Judicial proceedings continue.

- A joint investigation by the OIG's Miami Field Office and the Department of Housing and Urban Development (HUD) OIG resulted in the arrest of an FBI special services technician assigned to the FBI's Miami Division for making false statements and theft of government funds. A 39-count indictment returned in the Southern District of Florida alleged that, from January 2003 through December 2005, the special services technician received more than $24,000 in HUD Section 8 housing subsidies that she was not entitled to and provided false statements to HUD. The support services technician did not disclose her employment with the FBI in the housing subsidy application she submitted to HUD, thereby lowering the amount of income she reported to HUD. The support services technician would not have qualified for the housing subsidies if she had correctly reported her income. The FBI placed her on indefinite suspension without pay pending the outcome of the investigation. Judicial proceedings continue.

- The OIG confirmed allegations that an FBI special agent regularly frequented an adult entertainment club and accepted monetary, sexual, and other gratuities from the club owner and its employees over a 6-year period. OIG investigators also determined that the special agent allowed the club owner to use his FBI vehicle on at least two occasions and provided the owner with sensitive law enforcement information. The case was declined for prosecution by the Department's Public Integrity Section, and the OIG provided its report to the FBI for appropriate administrative action.

Ongoing Work

The FBI's Use of Certain Patriot Act Authorities

As required by the *USA Patriot Improvement and Reauthorization Act of 2005*, the OIG is reviewing the FBI's use of authorities modified under the

Patriot Act to obtain business records for foreign intelligence purposes and issue National Security Letters. Our review will examine the effectiveness of these investigative tools and identify any noteworthy circumstances related to their use. We also will examine what information was collected, retained, and analyzed, and how it was used and disseminated; any procedural delays that may have harmed national security; and any impediments that may have prevented the FBI from making full use of the authorities under the Patriot Act. The report is due to Congress by March 2007.

Sentinel Contract Review

In March 2005, the FBI announced plans to develop the Sentinel case management system to replace the failed Virtual Case File effort. The main goal of Sentinel is to enable the FBI to move from a paper-based reporting system to an electronic records system and maximize the FBI's ability to use and share the information in its possession. As the second in a series of audits evaluating the development and implementation of the FBI's Sentinel project, the OIG is reviewing the Sentinel contract to determine if it contains the necessary work requirements, benchmarks, and other provisions to help ensure the success of the project. The audit also will assess the FBI's progress in addressing the concerns discussed in our previous Sentinel audit report issued in March 2006. In addition, on September 14, 2006, the Inspector General testified before the House Appropriations Committee, Subcommittee on Science, the Departments of State, Justice, and Commerce, and Related Agencies, concerning "Oversight of the Federal Bureau of Investigation." His testimony focused on the FBI's Sentinel program and discussed the preliminary results of the OIG's second audit.

Follow-Up Review Examining Hanssen Review Recommendations

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

Follow-Up Review of the FBI's Control Over Weapons and Laptop Computers

In August 2002, the OIG issued several audit reports on the control of weapons and laptop computers by various Department components. These reports detailed significant lapses in the control of weapons and laptops, particularly in the FBI. Our follow-up audit will focus on the FBI's efforts to take corrective action on the recommendations in our original audit report.

Follow-Up Review of the FBI's Progress in Hiring, Training, and Retaining Intelligence Analysts

The OIG issued a report in May 2005 examining the FBI's efforts to hire, train, and retain intelligence analysts. The OIG report made 15 recommendations to help the FBI improve its efforts in this area. We currently are conducting a follow-up audit to examine the progress made by the FBI in response to these recommendations.

Review of the FBI's Investigation of Certain Domestic Advocacy Groups

The OIG initiated a review to examine allegations that the FBI targeted domestic advocacy groups for scrutiny based solely upon their exercise of rights guaranteed under the First Amendment. The review will examine allegations regarding the FBI's investigation, and the predication for any such investigation, of certain domestic advocacy groups, including the Thomas Merton Center, Greenpeace, and People for the Ethical Treatment of Animals. The review will be similar in scope to our review of the FBI's investigation of potential protesters at the 2004 Democratic and Republican National Conventions.

FBI Reports of Alleged Abuse of Military Detainees

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

Federal Bureau of Prisons

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

Reports Issued

The BOP's Monitoring of Mail for High-Risk Inmates

In March 2005, news media reported that three terrorists who were convicted for the 1993 World Trade Center bombing and incarcerated at the BOP's highest-security prison, the Administrative Maximum Facility (ADX) in Florence, Colorado, had written over 90 letters to Islamic extremists outside the prison between 2002 and 2004. These extremists included incarcerated members of a Spanish terror cell with links to other terrorists suspected in the March 2004 attacks on Madrid commuter trains, and other Islamic radicals in Spain and Morocco — among them a man charged with using the BOP inmates' letters for recruiting suicide operatives. As a result, the OIG's Evaluation and Inspections Division reviewed the BOP's efforts to prevent terrorists and other high-risk inmates from using the mail or the cover of a foreign language to continue or encourage terrorism or criminal activities.

The OIG review concluded that the BOP's monitoring of inmate mail and other forms of communication was deficient in several respects: 1) the BOP does not read all the mail for terrorists and other high–risk inmates on its mail monitoring lists, 2) the BOP does not have enough proficient translators to translate inmate mail written in foreign languages, and 3) the BOP does not have sufficient staff trained in intelligence techniques to analyze whether terrorists' communications contain suspicious content. In addition to the deficiencies in its mail monitoring efforts, the OIG also found that the BOP is unable to effectively monitor high-risk inmates' verbal communications, which include telephone calls, visits with family and friends, and cellblock conversations.

According to BOP officials, BOP staff is expected to read 100 percent of the mail for inmates placed on mail monitoring lists. However, staff members at 7 of the 10 institutions that we visited told us they were not reading 100 percent of the mail for inmates on mail monitoring lists, and the

percentage of mail read had decreased since FY 2005 due to staff reallocations.

BOP staff also randomly read the mail of inmates not on monitoring lists in order to gather intelligence. However, staff at seven institutions told us that the high volume of mail, short processing deadlines, and staff reallocations resulted in a decrease in the amount of random reading of inmate mail.

In addition, the OIG found that the BOP does not have adequate agency-wide procedures for translating inmate mail written in a foreign language. Instead, the BOP relies primarily on BOP staff volunteers to translate mail as a collateral duty. We also found shortcomings in the BOP's translation efforts, including: 1) the BOP does not ensure that the staff used to translate inmate communications meet language proficiency requirements, 2) the BOP does not have enough staff members fluent in foreign languages to provide necessary translations, and 3) BOP supervisors do not consistently support translating as a collateral duty for their staff.

To improve its handling of foreign language translations, the BOP recently hired three full-time language specialists. However, we found that the BOP has not provided the specialists with sufficient intelligence training to enable them to identify potential intelligence from communications that they translate.

In general, we found that the BOP's intelligence capability to analyze the contents of terrorist inmates' mail is not well developed. The BOP offers only limited intelligence training to its staff to enable them to identify suspicious content in the mail of terrorist inmates. For example, when staff members at ADX Florence learned that terrorist inmates had been corresponding with Islamic extremist inmates in Spanish prisons, the BOP did not notify the FBI because BOP staff members did not understand the implications of the correspondence in furthering terrorist activity.

The OIG also found that the BOP was not meeting its own internal goals for telephone monitoring of high-risk inmates, and thus, may be missing opportunities to gather intelligence about terrorism or criminal activity. In addition, we found that the Department does not have a policy requiring that all inmates arrested for international terrorism-related crimes be reviewed to determine whether they should be placed under Special Administrative Measures (SAMs), the most restrictive conditions that can be placed on an inmate's communications. We concluded that unless such a review is required, there is no guarantee that international terrorist inmates will receive the heightened security and communications monitoring they require during incarceration.

The OIG review also reported on the BOP's ongoing and proposed initiatives that should help improve the monitoring of communications for terrorists and other high-risk inmates. The BOP initiatives include building stronger foreign language translation and intelligence analysis capabilities through increased training of staff and use of electronic tools such as translation software, enhancing information sharing between its databases that contain information on inmate communications to facilitate intelligence analyses, consolidating terrorist inmates in a few institutions in order to concentrate the resources required to monitor them, limiting the volume of mail and other types of communication available to terrorists or other high-risk inmates, and attempting to eliminate unsolicited "junk mail" for inmates.

The OIG made 13 recommendations designed to strengthen these initiatives and provide additional improvements to the BOP's monitoring of mail and verbal communications of terrorists and high-risk inmates. Two additional recommendations

were addressed to the FBI and the Criminal Division. The BOP, Criminal Division, and FBI concurred with all 15 recommendations and have begun to develop plans to implement these recommendations.

Oversight of Department Expenditures Related to Hurricane Rita: Roof Repair at the Federal Correctional Complex in Beaumont, Texas

On June 23, 2006, the OIG issued an audit of the Department's expenditures for roof repair at the BOP Federal Correctional Complex in Beaumont, Texas. In October 2005, the BOP awarded a $5.18 million contract to D.K. Haney Construction, Inc., to repair or replace roofing damaged by Hurricane Rita. The BOP entered into the sole-source contract using FY 2006 hurricane supplemental funding. We found that: 1) the decision to use a sole source contract was appropriate, 2) the BOP took adequate steps to ensure that the contract was negotiated fairly and reasonably priced, and 3) the contract was awarded at an "arms length" basis.

Investigations

During this reporting period, the OIG received 2,804 complaints involving the BOP. The most common allegations made against BOP employees included job performance failure, use of unnecessary force, and rude or crude treatment of inmates. The vast majority of complaints dealt with non-criminal issues that the OIG referred to the BOP's Office of Internal Affairs.

At the close of the reporting period, the OIG had 238 open cases of alleged misconduct against BOP employees. The criminal investigations cover a wide range of allegations, including bribery, introduction of contraband, sexual abuse, and unnecessary use of force. The following are examples of cases involving the BOP that the OIG's Investigations Division investigated during this reporting period:

- A joint investigation by the OIG's Miami Field Office and the FBI led to the indictment of six BOP correctional officers assigned to the Federal Correctional Institution (FCI) in Tallahassee, Florida, on charges of conspiracy to sexually abuse female inmates and introduction of contraband. This is the case in which OIG Special Agent William "Buddy" Sentner III was killed in an exchange of gunfire initiated by one of the indicted correctional officers during the arrest operation.

  The OIG investigators developed evidence that the correctional officers were involved in a scheme to provide contraband to female inmates in exchange for sexual favors and money. According to the indictment, the defendants would conspire among themselves to switch duty assignments to facilitate this illegal sexual activity. The indictment further charges that the defendants conspired to cover up their illegal activities by requiring other female inmates to act as look-outs when the illegal sexual activity was taking place. The defendants kept inmates from reporting the defendants' illegal conduct by threatening to plant contraband among the inmates' belongings and by threatening to have the inmates transferred to a facility that was far from family members.

  In addition, the defendants showed victims information about the inmates on the BOP computer system as proof that the inmates could be tracked anywhere within the BOP system, and the defendants monitored telephone calls of specific inmates in order

to intimidate them and identify any inmates who were disclosing the defendants' criminal conduct. The defendants also asked other correctional officers and inmates to speak with individuals suspected of cooperating with law enforcement investigators in an attempt to persuade them not to cooperate. The 23-count indictment includes one count of conspiracy and multiple counts of mail fraud, bribery, and witness tampering. The indictment also seeks forfeitures of any proceeds the defendants received that are traceable to the criminal conduct. Two of the correctional officers pled guilty and are awaiting sentencing, three correctional officers are awaiting trial, and the sixth correctional officer was killed in an exchange of gunfire that he initiated during the execution of the arrest warrants.

- An investigation by the OIG's Chicago Field Office led to the arrest of two BOP correctional officers assigned to the FCI in Greenville, Illinois, on charges of deprivation of civil rights under color of law, conspiracy, aiding and abetting, and obstruction of justice. One of the correctional officers was additionally charged with making false statements. OIG investigators developed evidence that the correctional officers beat an inmate in his cell, blocked the views of surveillance cameras to conceal the incident, and made false entries in government documents. One of the correctional officers also provided a false affidavit to the OIG regarding how the inmate received his injuries. The case is being prosecuted by the Civil Rights Division and the U.S. Attorney's Office for the Southern District of Illinois. Judicial proceedings continue.

- Multiple investigations by the OIG's El Paso Area Office resulted in the arrest of five BOP contract correctional officers assigned to the Reeves County Detention Center in Pecos, Texas, on various charges, including bribery of a public official, providing or possessing contraband in prison, and sexual abuse of a ward. The investigations determined that three correctional officers accepted money from inmates in exchange for smuggling contraband into the detention center, a fourth correctional officer was sexually involved with an inmate, and a fifth correctional officer was sexually involved with an inmate and accepted money from him and other inmates for smuggling marijuana into the detention center. Three correctional officers pled guilty, and judicial proceedings continue for the other two. All five correctional officers have resigned.

- An investigation by the OIG's New York Field Office developed evidence that a BOP correctional officer provided contraband, including drugs, to inmates housed at the Metropolitan Correctional Center in New York in exchange for cash payments totaling $8,000. The correctional officer was sentenced in the Southern District of New York to 18 months' incarceration and 3 years' supervised release on charges of bribery and introduction of contraband.

- A joint investigation by the OIG's Houston Area Office and the DHS OIG led to the arrest of a BOP senior correctional officer assigned to the U.S. Penitentiary in Pollock, Louisiana, 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, the Red Cross, and other contributions. Judicial proceedings continue.

- A joint investigation by the OIG's Los Angeles Field Office and the FBI led to the arrest of a BOP correctional officer assigned to

the U.S. Penitentiary in Lompoc, California, on charges of bribery and introduction of contraband. During an undercover operation, the correctional officer accepted drugs, merchandise, and a cash bribe of $7,500 in exchange for smuggling contraband into the institution. The correctional officer resigned from his position. Judicial proceedings continue.

- A joint investigation by the OIG's Miami Field Office and the FBI led to the arrest of a BOP correctional officer assigned to the Federal Correctional Complex in Coleman, Florida, on a charge of conspiracy to possess with intent to distribute marijuana. The investigators developed evidence that the correctional officer provided an inmate with drugs and merchandise. During the investigation, the correctional officer met with an OIG undercover agent and accepted $2,000 for the delivery plus an additional $16,000 for future deliveries. The correctional officer resigned from her position as a result of the investigation. Judicial proceedings continue.

Procedural Reform Recommendation

The OIG prepares a Procedural Reform Recommendation (PRR) recommending corrective action by a Department component when an investigation identifies a systemic weakness in an internal policy, practice, procedure, or program. The following PRR was sent to the BOP during this reporting period:

The OIG investigated a Muslim inmate's allegation that BOP staff violated his civil rights and civil liberties by preventing him from praying in the library. Our investigation found that when the inmate questioned an instruction from a BOP staff member forbidding prayer in the library on the basis that the inmate had been allowed to pray in that location in the past, the inmate was punished for refusing to obey an order.

The OIG reviewed current BOP policies on prayer and found a lack of guidelines — specifically when and where inmates are allowed to pray aloud — that could create a perception of religious discrimination or violation of religious freedom and privacy because the matter is left to the discretion of individual staff members. The OIG recommended that the BOP consider developing policies, which may need to be institution specific, establishing when and where individual inmates may pray aloud or engage in other ritualized prayer. A response from the BOP to the PRR is pending.

Ongoing Work

Review of Health and Safety Issues at BOP Computer Recycling Facilities

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

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 primarily in 23 field divisions across the 50 states, Puerto Rico, the U.S. Virgin Islands, and Guam. Foreign offices are located in Mexico, Canada, Colombia, and France.

Reports Issued

Review of ATF's Violent Crime Impact Team Initiative

ATF began the Violent Crime Impact Team (VCIT) initiative in June 2004 with the goal of decreasing homicides and violent crimes committed with firearms in targeted urban areas. VCITs currently operate in 23 cities across the country, and the initiative is slated to expand by 15 additional cities by FY 2008. The VCIT strategy includes targeting specific geographic areas or "hot spots" with a high rate of firearms violence, targeting the "worst-of-the-worst" violent offenders in those areas, building effective working relationships with community leaders, using ATF firearms investigative technology resources, and involving representatives from other Department law enforcement components.

The OIG's Evaluation and Inspections Division examined ATF's implementation of the VCIT initiative and concluded that, while the strategy may be an effective tool to reduce violent crime in targeted areas, inconsistent oversight and direction from ATF Headquarters have allowed local VCITs to ignore key elements of the strategy. We also found that ATF's claim in January 2006 that it had met its stated goal was based on insufficient data.

Our report found that ATF did not consistently implement the VCIT strategy. For example, rather than target specific "hot spots," two VCITs targeted entire cities and another targeted an entire county — with the population in the VCIT target areas ranging from 25,000 to 3 million. None of the five VCITs that we visited actively participated in any community outreach, six VCITs did not compile a "worst-of-the worst" list, and seven did not keep their lists up to date. In addition, VCITs did not consistently use ATF's technology resources for their investigations and

frequently did not include representatives from other Department law enforcement components.

We also concluded that ATF could not support its claim in its January 2006 report on best practices that the number of homicides committed with firearms was lower in 13 of the 15 VCIT pilot cities' target areas compared to the same 6-month period the preceding year. For example, ATF used city-wide data rather than data limited to the target area that the VCIT was serving. In addition, rather than look at the total number of violent firearms crimes in a VCIT target area, ATF examined only the number of homicides committed with firearms — a number that was relatively small and not reliable for drawing conclusions about the effectiveness of the VCIT initiative.

We also found that ATF's conclusion that homicides with firearms were trending downward in the VCIT cities was not consistent with accepted standards for trend analysis because the time period ATF examined was too short to draw any conclusions about trends.

The OIG made five recommendations to improve ATF's implementation of the VCIT initiative, including establishing specific operational guidelines for VCIT implementation and developing an adequate evaluation strategy to assess the success of the VCIT program. ATF, while disagreeing with some of the findings in the OIG report, concurred with all five of our recommendations.

Investigation into Allegations of Mismanagement and Misconduct by the ATF Director

In September 2006, the OIG's Oversight and Review Division completed its report on allegations of mismanagement and misconduct by the former Director of ATF, who resigned in August 2006. The investigation was initiated in February 2006 after the OIG received an anonymous letter of complaint alleging that the former Director engaged in various acts of mismanagement.

The report details the results of our investigation, which substantiated several allegations in the complaint against the former Director. We reviewed the former Director's decisions regarding the construction of ATF's headquarters building and questioned several expenditures that he authorized in connection with that construction project, as well as other construction projects. We also found that the former Director's use of ATF resources for security was extensive and resulted in an unnecessary drain on resources, particularly when he traveled to field divisions.

In addition, while we found that the former Director did not commit travel abuse, we questioned certain expenditures and use of resources in connection with his overseas travel. For example, we had concerns about the number of travelers who accompanied the former Director on foreign travel and, in particular, the need for an extensive security detail to accompany him on one overseas trip.

We also found that the former Director violated ethics rules by directing ATF staff to assist his nephew in producing a video about ATF for his high school class project.

The former Director's written response to our report was appended to the final report.

ATF's Management of Seized Assets and Evidence

ATF seizes for forfeiture and evidentiary purposes items such as alcohol, tobacco, firearms, explosives, ammunition, vehicles, real property,

currency, and computer equipment. Between October 2003 and June 2006, ATF seized 240,802 items with an estimated fair market value of over $57 million. In September 2006, we completed an audit to determine the status of ATF's transition to the Department's automated system for managing seized assets and to assess the adequacy of ATF's accounting for, storing, safeguarding, and disposing of seized assets and evidence in its possession.

When ATF transferred to the Department from the Department of Treasury in January 2003, ATF's asset tracking system was not immediately migrated into the Department's asset tracking system because the Department was in the midst of a system upgrade. Our audit found that since ATF's transfer certain data fields in ATF's system have not been tracked in the Department's Consolidated Asset Tracking System (CATS), and that these issues must be resolved in order for system migration to be completed by its target date of June 2007. To accomplish this, ATF must provide appropriate supporting documentation to the Asset Forfeiture Management Staff about seized and forfeited assets and ensure that current and future funds still in the Treasury Department's Asset Forfeiture Fund can be promptly transferred to the Department's Asset Forfeiture Fund.

In addition, we found that ATF lacked a proactive contingency plan that addresses accounting for, storing, and safeguarding seized assets and evidence in the event of a natural disaster or other significant event.

We made five recommendations to assist ATF in meeting the requirements for completing its migration into CATS. ATF agreed with the recommendations and currently is implementing corrective action.

Ongoing Work

National Firearms Registration and Transfer Record

The OIG is reviewing ATF's National Firearms Registration and Transfer Record to determine whether ATF is effectively maintaining accurate and reliable records of registrations and transfers of *National Firearms Act* weapons.

Gun Shows

The OIG is reviewing ATF's enforcement policies and practices relating to illegal firearms trafficking at gun shows.

U.S. Marshals Service

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

Reports Issued

USMS Intergovernmental Service Agreements for Detention Facilities

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

- During this reporting period, we completed an audit of the IGA with the Multnomah County Sheriff's Office (MCSO) in Portland, Oregon. According to Multnomah County records, the MCSO was paid approximately $5 million for 12 months ending June 30, 2002, and $6.2 million for 12 months ending June 30, 2004. Based on our audit of actual costs and daily population, we determined that the MCSO records only supported a jail-day rate of $111.96 rather than the $115.90 rate that the MCSO used. Our findings resulted in questioned costs and a recommendation to remedy $655,525 from the overstated jail-day rate.

Investigations

During this reporting period, the OIG received 214 complaints involving the USMS. The most common allegations made against USMS employees included job performance failure, use of excessive force or other civil rights violations, and waste or mismanagement. The OIG opened 22 investigations and referred 187 other allegations to the USMS's Office of Internal Affairs.

At the close of the reporting period, the OIG had 25 open cases of alleged misconduct against USMS employees. The following is an example of a case involving the USMS that the OIG's Investigations Division investigated during this reporting period:

- An investigation by the OIG's Dallas Field Office led to the arrest, guilty plea, and sentencing of a former U.S. Marshal on misdemeanor charges of interfering and

impeding an investigation. OIG investigators determined that the U.S. Marshal, while traveling through a national forest, was stopped by an Arkansas Game and Fish Commission officer. The U.S. Marshal refused to obey the officer's verbal instructions and shoved the officer. In addition, the U.S. Marshal subsequently provided false statements to the OIG regarding the incident. The U.S. Marshal was ordered to pay a $2,000 fine pursuant to his guilty plea. The U.S. Marshal retired from the USMS.

Procedural Reform Recommendation

The following PRR was sent to the USMS during this reporting period:

An investigation by the OIG's Miami Field Office revealed deficiencies in a contract between the USMS and Fidelity Asset Management Solutions (Fidelity). Fidelity handles the majority of the functions related to managing the nationwide inventory of USMS forfeited real property. During an OIG investigation into the theft of private goods from within a vacant forfeited residence, we found that the USMS contract with Fidelity does not outline recordkeeping requirements for personal property not subject to forfeiture that is contained within forfeited real property. This deficiency prevented the USMS from fully accounting for the property stolen in this case.

We recommended that the USMS modify its contract with Fidelity to specify that the contractor is required to conduct a separate inventory of contents not subject to forfeiture when dealing with vacant forfeited real property. The separate inventory would ensure that: 1) the contractor's performance is consistent with USMS policies, 2) items not subject to forfeiture are accounted for in the event of theft, and 3) USMS is in compliance with federal regulations with regard to the management and disposal of abandoned or unclaimed property. A response from the USMS to the PRR is pending.

Ongoing Work

USMS Justice Prisoner and Alien Transportation System

The Justice Prisoner and Alien Transportation System (JPATS) transfers prisoners and aliens in federal custody within the United States and overseas; performs scheduling, security, and medical functions in support of prisoner transportation; and provides air transportation for the USMS's Witness Security Program and for federal government responses to crises such as the September 11, 2001, terrorism attacks and the hurricanes of 2005. Managed by the USMS, JPATS serves the BOP, USMS, military, U.S. Immigration and Customs Enforcement, and state and local law enforcement organizations. The OIG is evaluating the USMS's operation of JPATS.

Judicial Security

The OIG is reviewing the USMS's efforts to protect the federal judiciary. This is a follow-up review to our inspection in 2004 of the USMS's ability to assess threats and determine appropriate measures to protect members of the federal judiciary during high-threat trials and while they are away from the courthouse.

Audit of USMS's Workforce Composition

The OIG is conducting an audit of the USMS's workforce composition and its effect on organizational performance. As part of the audit, we will review issues related to the USMS's human resources department, including management, planning, training, and utilization.

Drug Enforcement Administration

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

Reports Issued

Follow-Up Review of the DEA's Efforts to Reduce the Diversion of Controlled Pharmaceuticals

The OIG's Evaluation and Inspections Division conducted a follow-up review to assess the DEA's actions to control pharmaceutical diversion. Controlled pharmaceuticals such as narcotics, stimulants, and depressants can be diverted from legitimate channels through theft or fraud during the manufacturing and distribution process. In recent years, the Internet also has emerged as a significant source for diverted pharmaceuticals, with hundreds of Internet pharmacies providing large amounts of pharmaceuticals to customers without a prescription.

Our follow-up review found that the DEA has taken important steps to improve its ability to control the diversion of pharmaceuticals, especially over the Internet. Those steps include making diversion control a strategic goal, establishing performance measures for diversion control, centralizing its diversion criminal investigations with other criminal investigations, and providing additional intelligence resources to diversion investigators. The DEA also has increased the number of authorized domestic diversion investigator positions from 512 in FY 2004 to 587 in FY 2005. In an effort to control the increasing use of the Internet to divert pharmaceuticals, the DEA has increased the time (from 3 to 11 percent) diversion investigators spend investigating Internet diversion cases and developed an operational strategy for Internet investigations that has been used successfully in several large pharmaceutical diversion operations.

Despite these positive actions, we found that several shortcomings persist that were first reported in our 2002 review. While criminal diversion investigations increased 23 percent from FYs 2002 to 2005, the time spent by special agents assisting diversion investigations still constitutes a small share of their total investigative effort. Special agent assistance is critical because diversion investigators lack law enforcement authority and must depend on DEA special agents or other law enforcement officers to perform tasks such as making arrests and serving search warrants. Further, the diversion groups in the field still receive only limited support from intelligence analysts, and intelligence analysts and

special agents are offered minimal diversion control training.

With respect to the DEA's Internet efforts, we found that: 1) the Online Investigations Project, under development since 2001, has become a valuable investigative tool even though it cannot automatically identify websites with the highest volume of suspect pharmaceutical sales as the project was originally intended; 2) telephone and online hotlines for reporting suspicious Internet pharmacies have yielded few leads that resulted in diversion investigations; 3) the distribution of undercover credit cards to diversion groups has been slow; and 4) more than half the diversion investigators who received training for Internet investigations said the training was inadequate.

We made six recommendations concerning special agent support for diversion investigations, diversion training for special agents and intelligence analysts, and implementation of the undercover credit card program. The DEA concurred with five of the six recommendations and has presented an action plan for addressing all the recommendations.

Investigations

During this reporting period, the OIG received 258 complaints involving the DEA. The most common allegations made against DEA employees included job performance failure, false statements, release of information, and misuse of a credit card. The OIG opened 4 investigations and referred 249 allegations to the DEA's Office of Professional Responsibility.

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

- In our March 2006 *Semiannual Report to Congress*, we reported on a case in which an investigation by the OIG's Miami Field Office led to the arrest of a former DEA special agent on charges that he submitted false expense vouchers for career fair expenses and received $13,405 that he was not entitled to. During this reporting period, the agent was sentenced to 3 years' probation and ordered to pay $13,405 in restitution and perform 250 hours of community service.

- A joint investigation by the OIG's Washington Field Office and the DEA's Office of Professional Responsibility led to the arrest and guilty plea of a DEA special agent assigned to the Richmond District Office on a charge of making false statements. The investigation disclosed that the special agent falsely denied having sexual relations with a female informant. He resigned as a result of the investigation. Sentencing is pending.

Ongoing Work

The DEA's International Operations

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

DEA Cash Seizures

In carrying out its mission, the DEA seizes cash assets that can be traceable to, or intended to be used for, illicit drug trafficking. The OIG is assessing the DEA's handling of its cash seizures.

Office of Justice Programs

OJP manages the Department's grant programs. OJP has about 700 employees and is composed of 5 bureaus — Bureau of Justice Assistance (BJA), Bureau of Justice Statistics, National Institute of Justice, Office of Juvenile Justice and Delinquency Prevention, and Office for Victims of Crime — as well as the Community Capacity Development Office.

Reports Issued

OJP Grants to State and Local Entities

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

- With its inception in FY 2002, the Southwest Border Prosecution Initiative (SWBPI) received $15.1 million through December 21, 2005, to reimburse state, county, parish, tribal, and municipal governments for costs associated with the prosecution of criminal cases referred by local USAOs. During our audit of the portion of the SWBPI that is administered by the New Mexico Department of Public Safety in Santa Fe, New Mexico, we questioned almost $1.1 million and made 20 recommendations based on the following deficiencies found in the claims reimbursed to the New Mexico Department of Public Safety: reimbursement was claimed for cases that were ineligible under the SWBPI guidelines, reimbursement amounts were calculated incorrectly based on case closure dates rather than resolution dates, and the number of cases claimed for reimbursement for each case disposition category did not always reconcile with the supporting documentation. OJP agreed with all of our recommendations and is in the process of coordinating corrective action with the New Mexico Department of Public Safety.

- The BJA Grant to the Delaware Judicial Branch, Wilmington, Delaware, provided nearly $1.8 million for the purchase of software licenses and implementation of services associated with deploying a case management system. Although the Delaware Judiciary generally complied with the grant requirements, we determined that it inappropriately charged this grant for maintenance expenditures not approved by the BJA. The Delaware Judiciary also did not develop performance measures that ensured the case management system would meet the goals and objectives of the project.

We made two recommendations to remedy questioned costs of $298,051 and ensure that performance measures are developed to assess whether the goals of the project are being met.

Investigations

During this reporting period, the OIG received 15 complaints involving OJP. The most common allegation made against OJP employees, contractors, or grantees was grantee fraud. The OIG opened eight investigations and referred five to OJP management.

At the close of the reporting period, the OIG had 18 open cases of alleged misconduct against OJP employees, contractors, or grantees. The following are examples of cases involving OJP that the OIG's Investigations Division investigated during this reporting period:

- A joint investigation by the OIG's Tucson Area Office, FBI, Internal Revenue Service's Criminal Investigative Division, HUD OIG, and Arizona Division of Occupational Safety and Health determined that the City of South Tucson, Arizona (City), made $86,652 in unsupported or unauthorized expenditures of OJP grant funds, including overcharging for salaries, commingling of grant funds with non-grant funds, and collecting unsupported overtime costs for police officers. In addition, the City violated Occupational Safety and Health regulations concerning the purchase, storage, and use of life support and training equipment for the City's fire department. The City has been directed to reimburse OJP $86,652 and has been fined $10,000 by the Arizona Division of Occupational Safety and Health.
- An investigation by the OIG's Fraud Detection Office led to disciplinary action against an OJP contracting specialist who accepted gratuities from a contractor. Investigators found that the contracting specialist engaged in improper personal contacts with a vendor, accepted high-value meals on multiple occasions, and improperly sought to influence the testimony of a witness when she learned that she was the subject of the investigation. The contracting specialist received a 45-day suspension, reassignment to a non-procurement position, and permanent revocation of her contracting warrant and was ordered to attend ethics and anger management classes as a result of the investigation.

Ongoing Work

State Criminal Alien Assistance Program

The OIG is conducting a congressionally mandated audit of the BJA's State Criminal Alien Assistance Program. Our audit will examine whether the states who receive compensation under section 241(i) of the *Immigration and Nationality Act* have fully cooperated with DHS's efforts to remove undocumented criminal aliens from the United States, and whether those states have policies that are in compliance with the Act. In addition, we will report on the number of criminal offenses committed by aliens unlawfully present in the United States after being apprehended by state or local law enforcement officials for a criminal offense and subsequently released without referral to the DHS for removal from the United States, including the number who were released because the state or political subdivision lacked space or funds for detention. Our findings are due to Congress by January 5, 2007.

Other Department Components

U.S. Attorneys' Offices

U.S. Attorneys serve as the federal government's principal criminal and civil litigators and conduct most of the trial work in which the United States is a party. Under the direction of the Attorney General, 93 U.S. Attorneys are stationed throughout the United States, Puerto Rico, the U.S. Virgin Islands, Guam, and the Northern Mariana Islands. More than 11,700 employees work in those offices and in the EOUSA.

Reports Issued

Allegations Relating to the Selection of the U.S. Attorney for Guam and the Northern Mariana Islands

In June 2006, the OIG's Oversight and Review Division issued its report regarding allegations raised by Frederick Black, the former interim U.S. attorney for Guam and the Commonwealth of the Northern Mariana Islands. Black alleged that he was replaced as the interim U.S. Attorney because he called for an investigation of Washington, D.C., lobbyist Jack Abramoff and because he supported applying federal immigration law to the Mariana Islands, a position Abramoff opposed.

Our investigation found that another person, Leonardo Rapadas, had already been chosen as the nominee for the U.S. Attorney's position in Guam pursuant to the normal selection process well before Abramoff tried to become involved in the process. We concluded that Abramoff played no role in the selection of Rapadas. However, when informed of the White House's decision to select Rapadas, Abramoff attempted to take credit with his Guam contacts for the selection, even though Abramoff had played no role in it.

Our report describes the selection process for the Guam U.S. Attorney position and the timing of key events in the process. We concluded that Black's call for an investigation of Abramoff was not related to his removal as interim U.S. Attorney, and that Abramoff did not have any influence on Rapadas's nomination. Moreover, we found that the Department offered to provide support for any investigation by Black's office regarding Abramoff, but Black acknowledged that he placed any such investigation on the "back burner" because of other ongoing investigations into alleged political corruption in Guam.

We also determined that Black's support for a recommendation contained in a May 2002 internal Department security report advocating the application of federal immigration law to the Northern Mariana Islands did not affect the

appointment of Rapadas because he had been selected as the U.S. Attorney nominee 2 months prior to the issuance of the report. In addition, we found no evidence suggesting that those involved in the selection of Rapadas were focused on this immigration issue.

Finally, the OIG report concluded that the evidence did not support a series of other allegations raised by Black, including that Rapadas's background investigation was insufficient or that the Guam USAO had abandoned public corruption investigations.

Ongoing Work

Critical Incident Response Plans

The OIG is conducting a follow-up review examining the progress made by USAOs with respect to improving their critical incident response plans in response to a December 2003 OIG review. The review also will assess whether the revised plans and accompanying policies provide sufficient preparation and guidance for the USAOs in critical incidents.

Civil Rights Division

Investigations

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

- An investigation by the OIG's Washington Field Office led to the arrest and guilty plea of a former Civil Rights Division trial attorney on a conflict of interest charge. OIG investigators determined that from February 2004 to June 2004 the trial attorney was employed as the lead attorney in the Department's investigation of a California juvenile correctional facility. While lead attorney, he negotiated for employment as a State of California Special Master where he would oversee California's reform of its juvenile facilities. He was sentenced to 1 year of probation and fined $3,000.

Criminal Division

Reports Issued

Equitable Sharing Grant Audits

The *Comprehensive Crime Control Act of 1984* granted the U.S. Attorney General the authority to share federally forfeited assets with cooperating local law enforcement agencies. The purpose of the Department's Forfeiture Program is to deter crime by depriving criminals the profits and proceeds of illegal activities while enhancing cooperation among federal, state, and local law enforcement agencies.

State and local law enforcement agencies receive equitable sharing assets when participating directly with Department 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. The amount of seized assets the USMS shares with agencies is generally calculated as a percentage of agency time spent participating in the investigation leading to an asset forfeiture.

During this reporting period, we audited the Baltimore County, Maryland, Police Department (BCPD) to assess whether equitable sharing assets received were accounted for properly and used for allowable purposes as defined by the applicable regulations and guidelines. We determined that equitable sharing funds enabled the BCPD to expand the use and mobility of its air and marine units, enhance its forensics laboratory operations, and provide additional communication capability via more mobile telephones and computer equipment upgrades. However, we found the BCPD could not provide adequate supporting documentation for expenditures totaling $100,173, and we questioned costs of $302,685. We developed 11 recommendations to remedy the questioned costs, require the BCPD to strengthen its procedures over the receipt and deposit of equitable sharing funds, and implement a policy of not projecting equitable sharing receipts for budget purposes.

Multicomponent Audits, Reviews, and Investigations

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

Reports Issued

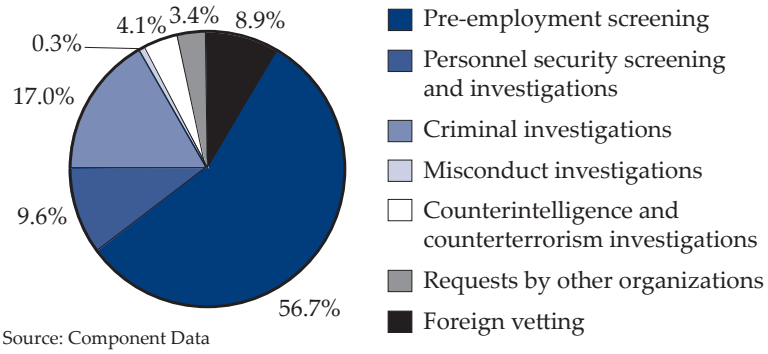
Use and Conduct of Polygraph Examinations in the Department

The OIG's Evaluation and Inspections Division examined the conduct and use of polygraph examinations in 11 Department components and the oversight mechanisms used to ensure that polygraphs are employed in accordance with established professional and technical standards. The review was an informational report that described the policies governing polygraph examinations in the Department and the situations under which Department employees are required to take the examinations.

As described in the report, some Department components have used polygraph examinations as a tool in criminal investigations and in some administrative misconduct investigations involving Department employees for over 70 years. In recent years, the use of polygraph examinations by the Department has expanded to include, among other usages, pre-employment screening, personnel security screening, and foreign counterintelligence and counterterrorism investigations (see Figure 1). From FY 2002 through 2005, the FBI, DEA, ATF, and OIG conducted more than 49,000 polygraph examinations. However, our review found no Department-wide policy concerning the conduct and use of polygraph examinations. Rather, each Department component has developed its own policies, procedures, and practices to govern polygraph examinations.

Within the Department the FBI is the only component with policies and procedures for compelling its employees to undergo polygraph examinations in personnel security and misconduct investigations. In addition, no other Department component has issued policies defining the circumstances under which employees can be compelled to submit to polygraph examinations in administrative misconduct investigations.

Figure 1: Purposes of Polygraph Examinations



Source: Component Data

The Department has periodically considered proposals to develop a Department-wide polygraph policy, but none has been acted upon to date. For example, in response to an OIG misconduct investigation in 2004, the Justice Management Division (JMD) stated that it believed, in the absence of a Department polygraph policy, that the Department could not compel Department employees to take a polygraph in a misconduct investigation. JMD proposed developing a Department polygraph policy, but the Department did not act on this proposal.

As part of this review, in June 2006 the OIG met with JMD officials to discuss whether the Department's position on compelled polygraphs had changed. JMD officials stated that it would reexamine whether the Department has the legal authority to compel employees to submit to polygraph examinations during investigations of administrative misconduct and, if so, what procedural steps would be required to exercise that authority.

The OIG report also provides information on several issues related to polygraph examinations, including the status of Executive Branch polygraph policy, the Office of Personnel Management's authorities for approving the use of polygraph examinations for competitive service employees, recent initiatives to establish standard federal polygraph policies and procedures, federal requirements for examiner training and certification, federal requirements for quality control and assurance reviews, the consequences of refusing or failing a polygraph examination, and the circumstances under which an employee can be compelled to submit to polygraph testing.

Civil Rights and Civil Liberties Complaints

Section 1001 of the Patriot Act directs the OIG to receive and review complaints of civil rights and civil liberties abuses by Department employees, to publicize how people can contact the OIG to file a complaint, and to submit a semiannual report to Congress discussing our implementation of these responsibilities. In August 2006, the OIG issued its ninth report summarizing its Section 1001 activities from January 1, 2006, to June 30, 2006.

The report described the number of complaints we received under this section, the cases that were opened for investigation, and the status of these cases. We also reported the findings from our investigation into allegations from an Egyptian national concerning alleged improper treatment during his arrest by the FBI on September 12, 2001, and his incarceration in a federal prison. This investigation revealed that several correctional officials violated BOP procedures in processing the male detainee into the facility by conducting a body cavity search that did not comply with BOP policy. We further found that the correctional officers later tried to conceal their role in this incident.

We also reported on the progress of our ongoing review of the FBI's use of two authorities amended by the Patriot Act: National Security Letters and requests for certain business records pursuant to Section 215 of the Patriot Act.

The Department's Information Security Program Pursuant to FISMA

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

For FY 2006, the OIG reviewed the security

programs of four Department components: the FBI, ATF, DEA, and JMD. Within these components, we selected for review three classified systems — JMD's Cyber Security Assessment and Management (CSAM) Trusted Agent-Secret, the FBI's System Security Information database, and the DEA's Merlin system — and two sensitive but unclassified systems — JMD's CSAM Trusted Agent and ATF's Headquarters Network Infrastructure. The OIG plans to issue separate reports in FY 2007 evaluating each of these systems.

On September 28, 2006, we submitted a response to the OMB questionnaire providing updated information on the overall effectiveness of the Department's IT security program. Our review disclosed that the Department had ensured that systems within the FBI, ATF, DEA, and JMD were all certified and accredited, system security controls were tested and evaluated within the past year, and system contingency plans were tested in accordance with FISMA policy and guidance. However, we found that electronic authentication risk assessments were not performed by the FBI, ATF, or DEA. We also found that the Department's plan of action and milestones process for tracking system vulnerabilities and corrective actions were not fully implemented in accordance with Department policy within the FBI and ATF. Moreover, Department-wide system configuration policy was not always implemented as required within the DEA and JMD. With respect to IT security awareness training, we found that ATF did not fully ensure that all of its employees were trained as required by Department policy.

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

Purchase Card Expenditures Related to Hurricane Katrina Recovery Efforts

In the aftermath of Hurricane Katrina, purchases using government purchase cards gained attention for weak internal controls that could result in improper and wasteful purchases, as well as missing and stolen assets. In September 2006, the OIG's Audit Division issued a report examining the $5.2 million in hurricane-related purchase card expenditures that the Department reported for August to December 31, 2005. The report described whether Department components: 1) employed effective internal controls over hurricane relief purchase card transactions to ensure that problems were minimized, 2) authorized and validated hurricane-related purchase card transactions, and 3) received the hurricane-related goods and services that were purchased.

We found that nearly all of the hurricane-related purchase card transactions tested were authorized

and valid, and the goods and services were received. However, the report identified internal control issues that should be corrected to ensure that future government funds are not at risk. The report found that for the FBI and ATF, the number of overall cardholders per administrative officer (also known as span of control) could significantly impact the oversight of a purchase card's use. In a previous OIG review, we recommended a span of control of no more than 7 cardholders per administrative officer, or a total of 300 transactions per month. Six of the eight components maintained an average span of control of four cardholders to one administrative officer.

However, ATF had on average 65 cardholders per administrative officer, with 23 administrative officers responsible for over 100 cardholders. The FBI had on average 23 cardholders per administrative officer, with 5 administrative officers responsible for 50 or more cardholders. In addition, we found that the FBI and ATF had administrative officers who were cardholders in the same group, which could allow the administrative officers to approve their own transactions. Further, we determined that approving officials and cardholders need refresher training that emphasizes prohibited purchases, requirements to document the availability of funds, and the importance of retaining adequate documentation.

The OIG made three recommendations: 1) ensure that a maximum span of control of 7 cardholders to 1 administrative officer, or a total of 300 transactions per month, is maintained; 2) reinforce policies on what items are not allowed to be purchased with purchase cards, the requirement to document the availability of funds, and the importance of retaining required supporting documentation; and 3) institute required purchase card refresher training at the FBI, ATF, USMS, and OJP. The Department generally concurred with the recommendations.

Accountability Organizations' Access to Information

The OIG's Evaluation and Inspections Division reported on issues that federal Offices of Inspector General and state and city audit organizations encountered in obtaining timely access to information — including documents and testimony — required to conduct evaluations, audits, and investigations. We also identified the most successful strategies used by accountability organizations for overcoming access problems. The review was initiated at the request of the Domestic Working Group, a group of federal, state, and local inspectors general and audit agencies organized under the auspices of the Government Accountability Office.

Our report, which summarized survey results from 128 accountability organizations, found that most survey respondents did not experience significant access problems in terms of denial of information. However, many organizations reported that they experienced delays in the receipt of information, which also can significantly hamper the effectiveness of their oversight work.

To overcome any access issues, survey respondents said they used a variety of strategies, including addressing issues early in the process, encouraging agency managers to support access to information, communicating frequently with agencies under review, and ensuring the protection of sensitive information.

Investigations

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

- A joint investigation by the OIG's Fraud

Detection Office and the New York Field Office led to the arrest of a painter at the World Trade Center on charges that he received more than $1 million from the September 11 Victim Compensation Fund based on his fraudulent claim that he was permanently disabled and unable to work as a result of back injuries sustained during the September 11 terrorism attacks. Videotape evidence gathered by the OIG demonstrated that the painter continued to engage in physical activities, such as bicycling and dancing, which were inconsistent with the injuries he claimed. In addition, the OIG found that the painter continued to paint houses in his neighborhood and fraudulently concealed from the hearing officer a back injury that he sustained in a motor vehicle accident that occurred prior to September 11, 2001. Judicial proceedings continue.

- An investigation by the OIG's Fraud Detection Office resulted in the County of York, Pennsylvania, agreeing to pay the United States $16 million to settle allegations under the *False Claims Act* that it knowingly submitted inflated claims to the former INS for housing INS detainees. The settlement arose from an intergovernmental services agreement between York and INS to house INS detainees in York County Prison. The parties entered into the agreement in 1995, and INS agreed to pay York $50 a day per detainee. In 2000, INS agreed to increase the rate to $60 a day based on York's certified statement of prison operating costs and its representation of the inmate population of the prison. In this statement, however, York inaccurately represented to INS that the average daily population of the prison was 996 inmates for the applicable period, rather than 1,544 as the county reported separately to the state. Understating the population allowed York to claim higher costs per inmate and thus increased the rate at which INS reimbursed York for housing federal detainees. This representation resulted in an inflated rate charged to the United States for detainees housed from October 1999 through March 2003. The OIG investigation, which arose from a referral by the OIG's Philadelphia Audit Office, was initiated prior to INS's transfer to the DHS.

Ongoing Work

Cost Tracking and Planning for Department IT Initiatives

In accordance with the requirements of the Department's FY 2006 Appropriations Conference Report, the OIG was directed to provide an inventory of major Department IT systems and report on research, plans, studies, and evaluations that the Department has produced, or is in the process of producing, concerning its information systems. In response, the OIG issued the first of three reports in March 2006: A report of the Department's major IT system investments by investment title/component, investment description, implementation status, and actual and projected costs. The second report will provide an audited verification of the information detailed in the unaudited report. The third report will detail the Department's research, plans, studies, and evaluations along with an analysis identifying the depth and scope of the problems the Department has experienced in the formulation of its IT plans.

Integrated Wireless Network

The Integrated Wireless Network (IWN) is intended to link approximately 80,000 federal, state, and local law enforcement officers and public safety agencies in a secure, interoperable wireless service that provides communications in support of law enforcement, first responder, and homeland security requirements. IWN currently

is a joint project of the Department, DHS, and the Department of the Treasury. The OIG is assessing the implementation of the IWN project, including its cost and deployment status.

The Department's Financial Statement Audits

The *Chief Financial Officers Act of 1990* and the *Government Management Reform Act of 1994* require annual financial statement audits of the Department. The OIG's Audit Division oversees and issues financial statement audit reports based on the work performed by independent public accountants. The FY 2006 financial statement audit currently is in process. The results will be included in the Department's FY 2006 Performance and Accountability Report, which is expected to be issued by November 15, 2006.

The Department's Internal Controls Over Terrorism Reporting

The Department measures its counterterrorism efforts in part by reporting terrorism-related statistics in its performance plans, budget requests, and statistical reports. An OIG audit is examining whether the Department and its components have adequate internal controls to ensure accurate reporting of terrorism-related statistics.

Violent Crime Task Force Coordination

At the direction of the House and Senate Appropriations Committees, the OIG is examining whether investigations conducted by four of the Department's violent crime task forces are well coordinated. Among other issues, the review will examine information-sharing efforts among the FBI's Safe Streets Task Forces, ATF's Violent Crime Impact Teams, DEA's Mobile Enforcement Teams, and USMS's Regional Fugitive Task Forces.

Information Security

The OIG has initiated a review to document the processes and requirements that Department components follow when investigating and reporting losses of sensitive information, including laptops containing sensitive or classified information.

Oversight of Intergovernmental Service Agreements

The OIG is conducting an audit of the USMS's and the Office of the Federal Detention Trustee's oversight of Intergovernmental Service Agreements (IGA), which are agreements with state and local prisons to house federal detainees awaiting trial or sentencing. Our objective is to determine if the USMS and the Office of the Federal Detention Trustee employ an effective monitoring and oversight process in light of the more than $755 million spent on IGAs in FY 2005.

Grant Closeout Process Utilized within the Department

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

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

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

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

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

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

Congressional Testimony

On September 14, 2006, the Inspector General testified before the House Appropriations Committee, Subcommittee on Science, the Departments of State, Justice, and Commerce, and Related Agencies, concerning "Oversight of the Federal Bureau of Investigation." His testimony focused on the FBI's Sentinel program, a multi-year project to upgrade the FBI's IT systems. He discussed the preliminary results of the OIG's second audit of Sentinel that examines the FBI's contracting for the project, including whether the FBI is establishing the necessary work requirements and baselines. The Inspector General testified that, although the OIG's current audit is not complete, preliminary findings indicate that the FBI has made progress toward resolving most of the OIG's initial concerns about planning for the Sentinel project. However, some concerns, such as the full staffing of the Sentinel Program Management Office, have not yet been fully addressed. Moreover, the current audit has identified additional issues that the OIG believes the FBI must resolve in order to avoid serious problems as the Sentinel project continues through its first phase of development and enters its more challenging and higher-risk second phase in early 2007. These issues include uncertainty over risk mitigation, contingency planning, and total project costs.

On August 3, 2006, the Counselor to the Inspector General testified before the National Prison Rape Elimination Commission regarding the OIG's efforts to vigorously investigate allegations concerning sexual abuse of inmates by federal correctional officers.

On May 2, 2006, the Inspector General testified before the Senate Committee on the Judiciary concerning "Oversight of the FBI." His testimony covered a variety of topics, including the FBI's efforts to upgrade its IT systems.

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 *ATF Modernization and Reform Act*, the *Intelligence Authorization Act for FY 2007*, and a proposal to provide penalties for the unauthorized disclosure of classified information were among the pieces of proposed legislation that the OIG reviewed.

Statistical Information

Audit Statistics

Audit Summary

During this reporting period, the Audit Division issued 105 audit reports containing more than $10 million in questioned costs and more than $3 million in funds to be put to better use, and made 335 recommendations for management improvements. Specifically, the Audit Division issued 11 internal reports of Department programs funded at more than $11 million; 24 external reports of contracts, grants, and other agreements funded at more that $102 million; and 70 *Single Audit Act* audits. In addition, the Audit Division issued six Notifications of Irregularities and one Management Improvement Memorandum.

Funds Recommended to Be Put to Better Use

Audit Reports	Number of Audit Reports	Funds Recommended to Be Put to Better Use
No management decision made by beginning of period	4	$6,870,284
Issued during period	5	$3,029,494
Needing management decision during period	9	$9,899,778
Management decisions made during period:		
◆ Amounts management agreed to put to better use[1]	5	$6,250,929
◆ Amounts management disagreed to put to better use	0	$0
No management decision at end of period	4	$3,648,849

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

Audits With Questioned Costs

Audit Reports	Number of Audit Reports	Total Questioned Costs (including unsupported costs)	Unsupported Costs
No management decision made by beginning of period	9	$13,072,142	$1,493,481
Issued during period	27	$10,366,537	$4,836,176
Needing management decision during period	36	$23,438,679	$6,329,657
Management decisions made during period:			
◆ Amount of disallowed costs[1]	23[2]	$13,042,412	$2,490,651
◆ Amount of costs not disallowed	0	$0	$0
No management decision at end of period	14	$10,396,267	$3,839,006

[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	10	30
Issued during period	94	335
Needing management decision during period	104	365
Management decisions made during period:		
◆ Number management agreed to implement[1]	79	292
◆ Number management disagreed with	0	0
No management decision at end of period	25	73

[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.

Audit Follow-Up

OMB Circular A-50

OMB Circular A-50, *Audit Follow-Up*, requires audit reports to be resolved within 6 months of the audit report issuance date. The Audit Division monitors the status of open audit reports to track the audit resolution and closure process. As of September 30, 2006, the OIG closed 95 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 September 30, 2006, the following audits had no management decision or were in disagreement:

- COPS Grants to the City of Camden, New Jersey
- COPS Grants to the Picuris Pueblo, New Mexico, Police Department
- COPS Grants to the Blackfeet Tribal Business Council, Montana
- COPS Grants to the Navajo Department of Resource Environment, Window Rock, Arizona
- COPS Grants to the AMTRAK Police Department
- COPS Grants to the Passamaquoddy Tribe and Pleasant Point Reservation Police Department, Perry, Maine
- FBI's Efforts to Prevent and Respond to Maritime Terrorism
- USMS Intergovernmental Service Agreement for Detention Facilities with the Central Virginia Regional Jail
- USMS Intergovernmental Service Agreement for Detention Facilities with the Blount County, Tennessee, Sheriff's Office
- USMS Intergovernmental Service Agreement for Detention Facilities with the Cumberland County Jail, Portland, Maine
- USMS Intergovernmental Service Agreement for Detention Facilities with the Western Tidewater Regional Jail, Suffolk, Virginia

Evaluation and Inspections Statistics

The chart below summarizes the Evaluation and Inspections Division's (E&I) accomplishments for the 6-month reporting period ending September 30, 2006.

E&I Workload Accomplishments	Number of Reviews
Reviews active at beginning of period	9
Reviews initiated	4
Final reports issued	6
Assistance in support of joint projects	1
Reviews active at end of reporting period	6

Unresolved Reviews

DOJ Order 2900.10, *Follow-up and Resolution Policy for Inspection Recommendations by the OIG*, requires reports to be resolved within 6 months of the report issuance date. As of September 30, 2006, one report, "Review of the Office of Justice Programs' Forensics Science Improvement Grant Program," had two unresolved recommendations. The OIG continues to work with OJP to resolve them.

Investigations Statistics

The following chart summarizes the workload and accomplishments of the Investigations Division during the 6-month period ending September 30, 2006.

Source of Allegations	
Hotline (telephone and mail)	1,062
Other sources	3,662
Total allegations received	4,724
Investigative Caseload	
Investigations opened this period	193
Investigations closed this period	202
Investigations in progress as of 9/30/06	374
Prosecutive Actions	
Criminal indictments/informations	83
Arrests	86
Convictions/Pleas	61
Administrative Actions	
Terminations	15
Resignations	59
Disciplinary action	15
Monetary Results	
Fines/Restitutions/Recoveries	$136,986
Seizures	$137,400
Civil penalties	$16 million

Integrity Awareness Briefings

OIG investigators conducted 202 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 9,000 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
BJA	Bureau of Justice Assistance
BOP	Federal Bureau of Prisons
CODIS	Combined DNA Index System
COPS	Office of Community Oriented Policing Services
DEA	Drug Enforcement Administration
Department	U.S. Department of Justice
DHS	Department of Homeland Security
EOUSA	Executive Office for U.S. Attorneys
FBI	Federal Bureau of Investigation
FISA	*Foreign Intelligence Surveillance Act*
FISMA	*Federal Information Security Management Act*
FY	Fiscal year
HUD	Department of Housing and Urban Development
INS	Immigration and Naturalization Service
IT	Information technology
JMD	Justice Management Division
OIG	Office of the Inspector General
OJP	Office of Justice Programs
OMB	Office of Management and Budget
Patriot Act	*USA PATRIOT Act*
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.

Loci: A specific location on a chromosome.

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.

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

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

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

Appendix 3

Evaluation and Inspections Division Reports

April 1, 2006 – September 30, 2006

Follow-Up Review of the DEA's Efforts to Control the Diversion of Controlled Pharmaceuticals

Review of ATF's Violent Crime Impact Team Initiative

Survey Results on Access to Information Problems Encountered by Federal, State, and Local Accountability Organizations

Follow-Up Review of the FBI's Progress Toward Biometric Interoperability Between IAFIS and IDENT

Use of Polygraph Examinations in the Department

The BOP's Monitoring of Mail for High-Risk Inmates

Appendix 4

Audit Division Reports

April 1, 2006 – September 30, 2006

INTERNAL AND EXTERNAL AUDIT REPORTS

BJA Democratic National Convention Security Grant to the City of Boston, Massachusetts

BJA Grant to the Delaware Judicial Branch, Wilmington, Delaware

Bureau of Justice Statistics Awards Administered by the National Opinion Research Center

BOP Medical Services Contract with John C. Lincoln Health Network, Phoenix, Arizona

CODIS Operational and Laboratory Vulnerabilities

Compliance with Standards Governing CODIS Activities at the Kansas Bureau of Investigation, Topeka DNA Laboratory

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

Compliance with Standards Governing CODIS Activities at the Massachusetts State Police Crime Laboratory, Sudbury, Massachusetts

Compliance with Standards Governing CODIS Activities at the Northern Regional Forensic Laboratory, Fairfax, Virginia

Compliance with Standards Governing CODIS Activities at the Tennessee Bureau of Investigation

Compliance with Standards Governing CODIS Activities at the Washoe County Science Division DNA Unit, Reno, Nevada

COPS Grants to the Assiniboine and Sioux Tribes Department of Public Safety, Poplar, Montana

COPS Homeland Security Overtime Grant to the Pennsylvania State Police

Department Purchase Card Expenditures Related to Hurricane Recovery Efforts

Independent Evaluation of the DEA's EPIC Information System — Classified — Pursuant to FISMA for FY 2005

Independent Evaluation of the DEA's EPIC Seizure System Pursuant to FISMA for FY 2005

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

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

Independent Evaluation of the BOP's Inmate Telephone System II Pursuant to FISMA for FY 2005

Management of Seized Assets and Evidence by ATF

OJP Methamphetamine Hot Spot Program Administered by the Missouri Department of Natural Resources

OJP No Suspect Casework DNA Backlog Reduction Program FY 2003 Cooperative Agreement Awarded to the Tennessee Bureau of Investigation

OJP Southwest Border Prosecution Initiative Administered by the New Mexico Department of Public Safety, Santa Fe, New Mexico

Office of Victims of Crime Grant and Cooperative Agreements to Justice Solutions

Oversight of Department Expenditures Related to Hurricane Rita: Roof Repair at the Federal Correctional Complex, Beaumont, Texas

Review of the FBI Headquarters' Information System Controls Environment for FY 2005

STOP Violence Against Women Formula Grant to the Arkansas Department of Finance and Administration

The FBI's Implementation of the Laboratory Information Management System

USMS Intergovernmental Service Agreement for Detention Services with the Hamilton County, Tennessee, Silverdale Correctional Facility

USMS Intergovernmental Service Agreement with the Multnomah County, Oregon, Sheriff's Office

Use of Equitable Sharing of Revenues by the AMTRAK Police Department

Use of Equitable Sharing of Revenues by the Baltimore City, Maryland, Police Department

Use of Equitable Sharing of Revenues by the Baltimore County, Maryland, Police Department

Use of Equitable Sharing of Revenues by the Los Angeles County, California, Sheriff's Department

Use of Equitable Sharing of Revenues by the St. Louis County, Missouri, Police Department

SINGLE AUDIT ACT REPORTS OF DEPARTMENT OF JUSTICE ACTIVITIES

April 1, 2006 – September 30, 2006

Acadiana Criminalistics Laboratory Commission, New Iberia, Louisiana

Alfond Youth Center and Affiliates, Waterville, Maine

Association of Missing and Exploited Children's Organization, Bronxville, New York

Calcasieu Parish Sheriff, Lake Charles, Louisiana

Catholic Charities of the Diocese of Galveston-Houston, Texas

Central City Economic Opportunity Corporation

City of Arlington, Texas, for FY 2003

City of Arlington, Texas, for FY 2004

City of Aurora, Colorado

City of Austin, Texas

City of Avondale, Arizona

City of Brenham, Texas

City of Bullhead City, Arizona

City of Chelsea, Massachusetts

City of Chester, Pennsylvania

City of Dallas, Texas

City of East Moline, Illinois

City of Fort Worth, Texas, for FY 2003

City of Fort Worth, Texas, for FY 2004

City of Gary, Indiana

City of Monroe, Louisiana

City of Odessa, Texas

City of St. Gabriel, Louisiana

City of Sunland Park, New Mexico

City of Texarkana, Texas

County of Merrimack, New Hampshire

County of Torrance, New Mexico

DA of the Orleans Judicial District

Dallas County, Texas

Excelsior College, Albany, New York

Guadalupe County, Texas

Harris County, Texas

Hidalgo County, Texas

Housing Authority of the City of Hugo, Oklahoma

Iberia Parish Sheriff, New Iberia, Louisiana

Jefferson Parish, Gretna, Louisiana

Juniata Valley Tri-County Drug and Alcohol Abuse Commission, Lewiston, Pennsylvania

Kickapoo Traditional Tribe of Texas, Eagle Pass, Texas

Lake County, Indiana

Little River Band of Ottawa Indians, Montana

Louisiana Foundation Against Sexual Assault, Inc., Independence, Louisiana

Municipality of Bluefield, West Virginia

National Association of Attorneys General

National Center for Victims of Crime

National Civic League of Colorado, Inc.

National Juvenile Detention Association, Inc.

Native American Alliance Foundation, Tulsa, Oklahoma

Oglala Sioux Tribe, South Dakota

Orleans Parish Juvenile Court, New Orleans, Louisiana

Our House, Inc., Monroe, Louisiana

Rosebud Sioux Tribe, South Dakota

SOS, Inc., Kansas

State of North Dakota

State of Texas for FY 2004

State of Texas for FY 2005

State of Wyoming for FY 2004

State of Wyoming for FY 2005

Tangipahoa Parish Sheriff, Amite, Louisiana, for FY 2003

Tangipahoa Parish Sheriff, Amite, Louisiana, for FY 2004

Tazewell County, Illinois

The Boys and Girls Club of Boston, Inc., Boston, Massachusetts

The Bridge Over Trouble Waters, Inc., Pasadena, Texas

The George Washington University

The Paul and Lisa Program, Essex, Connecticut

Tonto-Apache Tribe, Arizona

Town of North Reading, Massachusetts

Town of Winslow, Maine

United Keetoowah Band of Cherokee Indians of Oklahoma

Utica Neighborhood Housing Services, Inc., Utica, New York

Village of Carpentersville, Illinois

Audit Division Reports

April 1, 2006 — September 30, 2006

Quantifiable Potential Monetary Benefits

Audit Report	Questioned Costs	Unsupported Costs	Funds Put to Better Use
Acadiana Criminalistics Laboratory Commission, New Iberia, Louisiana	$82,672	$82,672	
BJA Democratic National Convention Security Grant to the City of Boston, Massachusetts	$74,965	$18,459	
BJA Grant to the Delaware Judicial Branch, Wilmington, Delaware	$298,051		
Bureau of Justice Statistics Awards Administered by the National Opinion Research Center	$11,295		
City of Arlington, Texas, for FY 2004	$872		
City of Austin, Texas	$13,985		
City of Gary, Indiana	$989,106	$988,883	
City of Sunland Park, New Mexico	$20,733		
COPS Grants to the Assiniboine and Sioux Tribes Department of Public Safety, Poplar, Montana	$2,799,475	$1,316,331	$79,840
COPS Homeland Security Overtime Grant to the Pennsylvania State Police	$251,308		$32,625
DA of the Orleans Judicial District	$1,278,970	$1,278,970	
Housing Authority of the City of Hugo, Oklahoma	$8,155	$8,155	
Kickapoo Traditional Tribe of Texas, Eagle Pass, Texas	$4,905	$4,905	
National Juvenile Detention Association, Inc.	$33,215		
Oglala Sioux Tribe, South Dakota	$877,605	$877,605	
OJP Methamphetamine Hot Spot Program Administered by the Missouri Department of Natural Resources	$1,799		

Audit Report	Questioned Costs	Unsupported Costs	Funds Put to Better Use
OJP No Suspect Casework DNA Backlog Reduction Program FY 2003 Cooperative Agreement Awarded to the Tennessee Bureau of Investigation			$2,832,208
OJP Southwest Border Prosecution Initiative Administered by the New Mexico Department of Public Safety, Santa Fe, New Mexico	$1,098,036	$42,270	
SOS, Inc., Kansas	$314	$314	
State of Texas for FY 2004	$830,130		
State of Texas for FY 2005	$205,224		
STOP Violence Against Women Formula Grant to the Arkansas Department of Finance and Administration	$94,731	$94,731	$68,535
Tangipahoa Parish Sheriff, Amite, Louisiana, for FY 2004	$19,688	$19,688	
Town of North Reading, Massachusetts	$155,240		
Use of Equitable Sharing of Revenues by the St. Louis County, Missouri, Police Department	$154,660		
Use of Equitable Sharing of Revenues by the AMTRAK Police Department	$3,020	$3,020	
Use of Equitable Sharing of Revenues by the Baltimore County, Maryland, Police Department	$402,858	$100,173	
USMS Intergovernmental Service Agreement for Detention Facilities with the Multnomah County, Oregon, Sheriff's Office	$655,525		
USMS Intergovernmental Service Agreement for Detention Services with the Hamilton County, Tennessee, Silverdale Correctional Facility			$16,286
Total	**$10,366,537**	**$4,836,176**	**$3,029,494**

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	42
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	7-41
Section 5(a)(2)	Significant Recommendations for Corrective Actions	7-40
Section 5(a)(3)	Prior Significant Recommendations Unimplemented	45-46
Section 5(a)(4)	Matters Referred to Prosecutive Authorities	14-15, 20-22, 26-27, 29, 31, 33, 38-39
Section 5(a)(5)	Refusal to Provide Information	None
Section 5(a)(6)	Listing of Audit Reports	50-54
Section 5(a)(7)	Summary of Significant Reports	7-40
Section 5(a)(8)	Audit Reports — Questioned Costs	44
Section 5(a)(9)	Audit Reports — Funds to Be Put to Better Use	43
Section 5(a)(10)	Prior Audit Reports Unresolved	45
Section 5(a)(11)	Significant Revised Management Decisions	None
Section 5(a)(12)	Significant Management Decisions with which the OIG Disagreed	None

Report Waste, Fraud, Abuse, or Misconduct

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

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

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

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

Report Violations of Civil Rights and Civil Liberties

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

Civil Rights and Civil Liberties Complaints
Office of the Inspector General

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

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

On-Line Report Availability

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

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

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

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

Or call: (202) 616-4550

In Memory of OIG Special Agent

William "Buddy" Sentner III

OIG Special Agent William "Buddy" Sentner III was shot and killed in the line of duty on June 21, 2006. Agent Sentner was working as part of an OIG and FBI team to execute arrest warrants on six BOP Correctional Officers at the Federal Correctional Institution in Tallahassee, Florida. The Correctional Officers were indicted on charges of conspiracy to sexually abuse female inmates and introduction of contraband.

As part of his remarks at Agent Sentner's funeral, Inspector General Glenn Fine described Buddy Sentner's heroic actions as follows:

"When a correctional officer who was being arrested opened fire, Buddy returned fire and acted with extraordinary courage. I believe that Buddy's brave actions under fire saved the lives of several other federal employees, while giving his own life. Buddy Sentner lived like a hero and he died as a hero."

Agent Sentner joined the OIG's San Diego Field Office in July 2002, and he transferred to the OIG in Coleman, Florida, in August 2003. While with the OIG, Agent Sentner worked as both a polygrapher and a criminal investigator. Agent Sentner graduated from the University of Maryland with a B.A. in criminology in 1987, and he conducted his graduate work in public policy at Georgetown University. Agent Sentner is survived by his wife, parents, and two siblings.

OIG Special Agent
William "Buddy" Sentner III
Killed in the Line of Duty
June 21, 2006

Agent Sentner was the first Department of Justice OIG agent killed in the line of duty. On September 12, 2006, the Attorney General's Award for Exceptional Heroism was awarded posthumously to Buddy Sentner in recognition of the exceptional courage he displayed by saving the lives of fellow officers. On October 24, 2006, the President's Council on Integrity and Efficiency/Executive Council on Integrity and Efficiency presented the first "Sentner Award for Dedication and Courage" posthumously to Buddy Sentner.

The OIG will always remember and be grateful for Agent Sentner's dedication and the sacrifice he made in service to his colleagues and his country. He was a deeply committed federal law enforcement agent, colleague, and friend. He will be greatly missed.

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

Established April 14, 1989