

# Office of the Inspector General

## Semiannual Report to Congress



April 1, 2003–September 30, 2003



## U.S. Department of Justice

Office of the Inspector General

---

# Message From the Inspector General

This year marks the 25<sup>th</sup> Anniversary of the *Inspector General Act* (IG Act). This legislation established in many Cabinet agencies Inspectors General who are responsible for detecting and deterring waste, fraud, and abuse, and promoting economy and efficiency. In 1988, the IG Act was amended to establish an Inspector General (IG) in the Department of Justice (Department), and the Department's Office of the Inspector General (OIG) began operation in April 1989.

Since its creation, the Department's OIG has consistently demonstrated its value in providing independent oversight of Department programs and personnel. During the past 14 years, the OIG has conducted hundreds of audits, evaluations, investigations, and special reviews that have helped improve the operation of the Department. During this time, our work has earned widespread recognition from within the Department, from Congress, and from the public. This success is attributable to the hard work and dedication of OIG employees throughout the years.

Our office's record of accomplishment has continued in recent years. We have aggressively and systematically undertaken additional responsibilities given to us by the Attorney General and by Congress, including expansion in 2001 of our authority to investigate allegations of misconduct in the Federal Bureau of Investigation (FBI) and the Drug Enforcement Administration (DEA) and added responsibilities under the *USA PATRIOT Act* (Patriot Act).

As reflected in this semiannual report, we continue to investigate serious allegations of misconduct in the FBI and DEA as well as complaints of civil rights and civil liberties abuses. Our audits and evaluations include comprehensive reviews of Department financial statements, computer security, information technology acquisitions, grants and contracts, and a variety of other Department programs.

Two special reviews completed this reporting period deserve special mention. In June 2003, we released a review of the treatment of aliens held on immigration charges in connection with the September 11 terrorist attacks. In August 2003, we completed a review of the FBI's performance in detecting, deterring, and investigating the espionage of FBI agent Robert Hanssen. Both reports were comprehensive assessments of sensitive issues, and both provided numerous recommendations for improvement. In response to both, the Department and the FBI agreed to take action to address our recommendations.

I am gratified by the support we are receiving for our work, both from the Attorney General and from Congress. The Attorney General regularly expresses his understanding of the role we play in helping improve the Department, and Congress has expressed confidence in us by providing additional responsibilities and resources. We appreciate this support and look forward to continuing to meet our critical responsibilities in the years ahead.

A handwritten signature in cursive script that reads "Glenn A. Fine".

Glenn A. Fine  
Inspector General  
October 31, 2003



# Table of Contents

<b>Highlights of OIG Activities</b> . . . . .	<b>1</b>
<b>OIG Profile</b> . . . . .	<b>3</b>
<b>Multicomponent Audits, Reviews, and Investigations</b> . . . . .	<b>5</b>
<b>The Federal Bureau of Investigation</b> . . . . .	<b>17</b>
<b>The Federal Bureau of Prisons</b> . . . . .	<b>22</b>
<b>The Drug Enforcement Administration</b> . . . . .	<b>26</b>
<b>Other Department Components</b> . . . . .	<b>28</b>
U.S. Marshals Service . . . . .	<b>28</b>
U.S. Attorneys' Offices . . . . .	<b>29</b>
Bureau of Alcohol, Tobacco, Firearms and Explosives . . . . .	<b>29</b>
<b>Top Management Challenges</b> . . . . .	<b>30</b>
<b>Congressional Testimony</b> . . . . .	<b>31</b>
<b>Legislation and Regulations</b> . . . . .	<b>31</b>
<b>Statistical Information</b> . . . . .	<b>32</b>
<b>Audit Statistics</b> . . . . .	<b>32</b>
Funds Recommended for Better Use . . . . .	<b>32</b>
Questioned Costs . . . . .	<b>33</b>
Management Improvements . . . . .	<b>33</b>
Audit Follow-Up. . . . .	<b>34</b>
Unresolved Audits . . . . .	<b>34</b>
Unresolved Inspections . . . . .	<b>34</b>
<b>Investigations Statistics</b> . . . . .	<b>35</b>
Sources of Allegations . . . . .	<b>35</b>
Investigative Caseload . . . . .	<b>35</b>
Prosecutive Actions . . . . .	<b>35</b>
Administrative Actions . . . . .	<b>35</b>
Monetary Results . . . . .	<b>35</b>

## Appendices

Audit Division Reports . . . . .	<b>36</b>
Glossary of Terms . . . . .	<b>47</b>
Acronyms and Abbreviations . . . . .	<b>48</b>
Reporting Requirements Index . . . . .	<b>49</b>



# 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 – September 30, 2003

Allegations Received by the Investigations Division	3,895
Investigations Opened	225
Investigations Closed	272
Arrests	83
Indictments/Informations	71
Convictions/Pleas	74
Administrative Actions	86
Fines/Restitutions/Recoveries	\$1.29 million
Audit Reports Issued	238
Questioned Costs	\$25.61 million
Funds Put to Better Use	\$1.50 million
Recommendations for Management Improvements	313

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

- ◆ **Treatment of September 11 Detainees.** The OIG reviewed the treatment of 762 aliens detained on immigration charges in connection with the FBI's September 11 terrorism investigation, including their processing, bond decisions, the timing of their removal from the United States or their release from custody, their access to counsel, and the conditions of their confinement. While the Department faced unprecedented challenges in responding to

the terrorist attacks, we found significant problems in how it handled these detainees. For example, in New York City little attempt was made to distinguish between aliens suspected of terrorism from those encountered coincidentally to the FBI's investigation. We found delays in providing charging documents that made it difficult for detainees to understand why they were being held, to obtain legal counsel, and to request a bond hearing. In one facility, where many detainees were held, we found unduly harsh conditions of confinement and physical and verbal abuse by some correctional officers against some detainees. We made 21 recommendations to improve the handling of detainees in future situations.

- ◆ **The FBI's Performance in the Hanssen Case.** This comprehensive review by the OIG examined the FBI's efforts to uncover the espionage of FBI agent Robert Hanssen, who compromised some of the nation's most important counterintelligence and military secrets until his arrest in February 2001. We concluded Hanssen escaped detection not because he was extraordinarily clever and crafty, but because of long-standing systemic problems in the FBI's counterintelligence program and a deeply flawed internal security program. The OIG made 21 recommendations to help the FBI improve its internal security and its ability to deter and detect espionage in its midst.
- ◆ **The FBI's Implementation of IT Recommendations.** Since 1990, OIG reports have cited numerous deficiencies in the FBI's information technology (IT) system, including outdated infrastructure, fragmented management, and inadequate training. In reviewing the FBI's efforts to implement past OIG recommendations, we found that although it had acted on many recommendations, further actions were needed in crucial areas such as management controls and security of the FBI's IT program.

- ◆ **FBI Casework and Human Resource Allocation.** This OIG audit found although the FBI had identified combating terrorism as its top priority in 1998, until the September 11 attacks it had devoted significantly more of its resources to traditional law enforcement activities than to its counterterrorism programs. We concluded the FBI needs to improve how it assesses and aligns its resources with its priorities.
- ◆ **Integrating Fingerprint Systems.** In the OIG's most recent review of efforts to integrate the computerized fingerprint identification systems of the FBI and the Immigration and Naturalization Service (INS), we found the project, already behind schedule, is likely to experience further delays.
- ◆ **The DEA's Performance-Based Management Efforts.** This OIG review found the DEA had failed to meet key aspects of the *Government Performance and Results Act of 1993* (GPRA). The DEA's strategic goal and objectives were not definitive enough to allow progress toward meeting them to be assessed; realistic performance goals were lacking; and an effective system for collecting, analyzing, and verifying performance data was needed.

### Investigations of Misconduct

As shown in the statistics in the table at the beginning of this section, the OIG investigates hundreds of allegations of misconduct. Examples of OIG investigations discussed in this report include:

- ◆ An FBI language specialist was arrested for unauthorized access of a computer for financial gain, making false statements, and trafficking in and using fraudulently obtained cellular phones. He pled guilty and was sentenced to five years' incarceration and three years' supervised release.
- ◆ A senior correctional officer in the Federal Bureau of Prisons (BOP) admitted to abusing a Muslim inmate by making derogatory racial, ethnic, and religious slurs and to providing an investigator with a "less than completely candid" memorandum concerning the incidents.
- ◆ A BOP correctional counselor was sentenced to 57 months' incarceration and 2 years' supervised release for accepting \$5,000 from an undercover police officer for smuggling narcotics into the prison.
- ◆ A deputy U.S. marshal who sold family members and friends vehicles and real estate that had been forfeited to the U.S. government was convicted of conspiring to defraud the United States, making false statements, embezzlement, and mail fraud.
- ◆ The former police chief of Kendleton, Texas, was indicted for conspiracy, wire fraud, and interference with commerce for allegedly defrauding a Department grant program by diverting a portion of the \$200,000 earmarked for hiring six new police officers to instead pay his own salary.

### Ongoing Reviews

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

- ◆ The FBI Laboratory DNA Analysis Unit's protocols and procedures.
- ◆ The effectiveness of the FBI's Legal Attaché program.
- ◆ The BOP's process for selecting the Muslim personnel, contractors, and volunteers who provide religious services to inmates.
- ◆ The DEA's process for investigating and disciplining employee misconduct.
- ◆ The development and effectiveness of the U.S. Attorneys' Offices' (USAOs) critical incident response plans.
- ◆ The effectiveness of the Federal Firearms Licensee Inspection Program.
- ◆ The priorities, functions, and accomplishments of the Department's counterterrorism task forces.

# 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 to promote economy and efficiency in Department operations. It 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; U.S. Marshals Service (USMS); Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); USAOs; and all other organizations in the Department.

The OIG consists of the Immediate Office of the IG and the following divisions and offices.

- ◆ **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 that govern 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 Washington Field Office and the Fraud Detection Office). It 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, and Policy and Administration.

- ◆ **Evaluation and Inspections Division** provides an alternative mechanism to traditional audits and investigations to review Department programs and activities.
- ◆ **Office of Oversight and Review** blends the skills of attorneys, investigators, and program analysts to investigate or review sensitive matters involving Department programs or employees.
- ◆ **Management and Planning Division** assists OIG components in the full range of human, material, and information resource areas by providing services in budget formulation and execution, security, personnel, training, travel, procurement, property management, information technology, computer network communications, telecommunications, strategic planning, and quality assurance and internal controls.
- ◆ **Office of General Counsel** provides legal advice to OIG management and staff. In addition, the office 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.

For the period covered by this *Semiannual Report to Congress* (report) – April 1 through September 30, 2003 – the OIG carried out its mission with a nationwide workforce of approximately 400 special agents, auditors, inspectors, attorneys, and support staff. For fiscal year (FY) 2003, following the transfer of \$1.10 million and 15 full-time equivalents to the Department of Homeland Security (DHS) as a result of the transfer of the INS from the Department to the DHS and the creation of the DHS's OIG, the OIG received \$56.45 million in direct appropriations and



earned an additional \$3.636 million in reimbursements. The OIG also received \$2.50 million from Public Law 108-11, the *Emergency Wartime Supplemental Appropriations Act, 2003*, funds that remain available until September 30, 2004.

As required by Section 5 of the IG Act, as amended, this report, reviewing the accomplishments of the OIG for the 6-month period ending September 30, 2003, is to be submitted no later than October 31, 2003, to the Attorney General for his review. The Attorney General is required to forward the report to Congress no later than

November 30, 2003, along with information regarding the Department's position on audit resolution and follow-up activity in response to matters discussed in this report.

**Information about the OIG and full-text versions of many of its reports are available at [www.usdoj.gov/oig](http://www.usdoj.gov/oig).**



**Audit and Investigations Divisions Locations  
as of September 30, 2003**

- Audit and Investigations Divisions Location
- Investigations Division Location Only

# Multicomponent Audits, Reviews, and Investigations

## Reports Issued

### Treatment of September 11 Detainees

After the September 11 terrorist attacks, the Department used federal immigration laws to detain aliens in the United States who were suspected of having ties to the attacks or connections to terrorism or who were encountered during the course of the FBI's investigation into the attacks. In the 11 months after the attacks, 762 aliens were detained in connection with the FBI's terrorism investigation on various immigration offenses, including overstaying their visas and entering the country illegally.

In furtherance of its responsibilities under the Patriot Act, the OIG examined the treatment of these detainees, including their processing, bond decisions, the timing of their removal from the United States or their release from custody, their access to counsel, and their conditions of confinement. The OIG's 198-page report, released in June 2003, focused in particular on detainees held at the BOP's Metropolitan Detention Center (MDC) in Brooklyn, New York, and at the Passaic County Jail (Passaic) in Paterson, New Jersey, a county facility under contract with the INS to house federal immigration detainees. We chose these two facilities because they held the majority of September 11 detainees and were the focus of many complaints of detainee mistreatment.

In response to the September 11 attacks, the FBI allocated massive resources to its terrorism investigation. In addition, the amount of information and leads about the attacks the FBI received in the weeks after the attacks was staggering. As our report pointed out, the Department was faced with unprecedented challenges responding to the attacks, including the chaos caused by the attacks and the possibility of follow-up attacks. Yet, while

recognizing these difficulties and challenges, we found significant problems in the way the Department handled the September 11 detainees.

Among the report's findings:

- ◆ The FBI in New York City made little attempt to distinguish between aliens who were subjects of its terrorism investigation (called "PENTTBOM") and those encountered coincidentally to a PENTTBOM lead. The OIG concluded that even in the chaotic aftermath of the September 11 attacks, the FBI should have expended more effort to distinguish between aliens who it actually suspected of having a connection to terrorism from those aliens who, while possibly guilty of violating federal immigration law, had no connection to terrorism but simply were encountered in connection with a PENTTBOM lead.
- ◆ The INS did not consistently serve the September 11 detainees with notice of the charges under which they were being held within the INS's stated goal of 72 hours. The review found that some detainees did not receive these charging documents for weeks, in some instances not for more than a month, after being arrested. These delays affected the detainees' ability to understand why they were being held, obtain legal counsel, and request a bond hearing.
- ◆ The Department instituted a policy that all aliens in whom the FBI had an interest in connection with the PENTTBOM investigation required clearance by the FBI of any connection to terrorism before they could be removed or released. The policy was based on the belief – which turned out to be erroneous – that the FBI's clearance process would proceed quickly. The OIG review found instead of taking a few days as anticipated, the FBI clearance process

took an average of 80 days, primarily because it was understaffed and not given sufficient priority by the FBI.

- ◆ In the first 11 months after the terrorist attacks, 84 September 11 detainees were housed at the MDC in Brooklyn under highly restrictive conditions. These conditions included “lock down” for at least 23 hours a day; escort procedures that included a “four-man hold” with handcuffs, leg irons, and heavy chains when the detainees were moved outside their cells; and a limit of one legal telephone call a week and one social call a month.
- ◆ BOP officials imposed a communications blackout for September 11 detainees immediately after the terrorist attacks that lasted several weeks. After the blackout ended, the MDC’s designation of the September 11 detainees as “Witness Security” inmates frustrated efforts by detainees’ attorneys, families, and even law enforcement officials to determine where the detainees were being held. We found MDC staff frequently – and mistakenly – told people who inquired about a specific detainee that the detainee was not held at the facility when, in fact, the opposite was true.
- ◆ With regard to allegations of abuse at the MDC, the evidence indicated a pattern of physical and verbal abuse by some correctional officers against some detainees, particularly during the first months after the attacks and during intake and movement of prisoners. Although the allegations of abuse have been declined for criminal prosecution, the OIG is continuing to investigate these matters administratively.
- ◆ By contrast, the OIG review found the detainees confined at Passaic had much different, and significantly less harsh, experiences than the MDC detainees did. According to INS data, Passaic housed 400 September 11 detainees from the date of the terrorist attacks through May 30, 2002 – the largest number of September 11 detainees held at any single U.S. detention facility. Passaic detainees housed in the general population were treated like “regular” INS detainees who also were held at the facility. Although we received some allegations of physical and verbal abuse, we did not find

the evidence indicated a pattern of abuse at Passaic.

- ◆ The OIG report made 21 recommendations to the relevant agencies, including the FBI and the BOP as well as the DHS’s Bureau of Immigration and Customs Enforcement. The recommendations dealt with issues such as developing uniform arrest and detainee classification policies, improving information-sharing among federal agencies on detainee issues, improving the FBI clearance process, clarifying procedures for processing detainee cases, revising BOP procedures for confining aliens arrested on immigration charges who are suspected of having ties to terrorism, and improving oversight of detainees housed in contract facilities. The OIG has received and analyzed responses to all of the recommendations. In general, the agencies agreed with the recommendations. Implementation of most of them is ongoing, and the OIG continues to monitor and report on the progress being made.

### Civil Rights and Civil Liberties Abuses

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 July 2003, the OIG issued its third Section 1001 report summarizing our Patriot Act-related activities from December 16, 2002, through June 15, 2003.

The report described the status of OIG and Department investigations of alleged civil rights and civil liberties abuses by Department employees. In addition, the report highlighted several OIG reviews undertaken in furtherance of our Section 1001 responsibilities, including the review examining the treatment of September 11 detainees held on immigration charges in connection with the terrorist attacks.

### Texas Legislators

On May 11, 2003, over 50 members of the Texas legislature left Texas to prevent a quorum in the Texas House of Representatives so that a pro-

posed redistricting plan could not be voted on. At the request of members of Congress, the OIG investigated whether any Department employees were involved in or any resources expended on efforts to locate and return the missing legislators. The OIG determined that Department employees in Washington, D.C., the FBI offices in Texas and Oklahoma, and the USAO in the Western District of Texas received various inquiries and requests for assistance in connection with the absent Texas legislators. These requests came from a variety of sources, including a member of U.S. House Majority Leader Tom DeLay's staff, members of the Texas Attorney General's office, and a member of the Texas Rangers. We found that in response to these requests Department employees, with one exception, appropriately recognized that this was a state matter and did not provide any assistance to the search for the Texas legislators.

In one instance, an FBI special agent in Texas received a request for assistance from an employee of the Texas Department of Public Safety (DPS) who was searching for two of the absent legislators. To assist the DPS officer, the FBI special agent made two calls to the cell phone of an absent legislator and determined that the legislator and another absent legislator were in Oklahoma. The FBI special agent relayed this information to the DPS officer.

The OIG concluded the FBI agent should have declined the request for assistance from the DPS employee but that he did not commit misconduct or violate any FBI policy. However, the OIG recommended the FBI examine the written guidance it provides to its agents about how to respond to requests for assistance from local law enforcement.

### **Streamlining of COPS and OJP Administrative Activities and Grant Functions**

To identify activities and functions that could be streamlined to increase the operational efficiency of the Department's federal financial assistance programs, we conducted an audit of the two offices primarily responsible for managing those programs: the Office of Justice Programs (OJP) and the Office of Community Oriented Policing

Services (COPS). We concluded that the Department's assistance programs are fragmented, resulting in reduced efficiency and higher costs to award and administer federal financial assistance funds to state and local agencies.

During the last several years, the Department's federal financial assistance programs have grown substantially in number and dollar value, reaching approximately \$5 billion for FY 2002. Since COPS was created in 1994, it has relied on OJP to perform services related to the COPS program. In recent years, COPS's management and administration (M&A) costs per program dollar have been higher than OJP's. COPS's M&A costs per grant administered have increased, while OJP's have decreased. Moreover, we determined that COPS grants for hiring personnel and purchasing equipment and grants awarded by OJP under the Local Law Enforcement Block Grants program overlapped and that no formal coordination existed between COPS and OJP to ensure that grantees did not receive funds for similar purposes from both agencies. We also found that COPS had not developed a capability to receive grant applications online and to download the application information directly into its grant management system. Instead, grantees must submit applications on paper, and COPS must manually input the data.

Since OJP was established in 1984, it has experienced dramatic growth that has included many new financial assistance programs created by Congress. Many of these programs overlap and have caused duplication and inefficiency within OJP. OJP management has developed a reorganization plan to improve OJP's efficiency and effectiveness in awarding and administering federal financial assistance programs. We concluded, however, that even after implementation of the plan, some duplication between grants awarded by different OJP offices will remain and some inefficiencies will not be fully addressed. For example, we found that OJP does not have a fully effective automated system to manage its grants or the capability for all potential grantees to apply for grants online.

Our report contains eight recommendations, including improving the coordination between COPS and OJP to eliminate duplication of effort

and ensure that awards are not made to the same grantee for similar purposes. COPS and OJP agreed with our recommendations and are in the process of implementing corrective actions.

### **Integration of the INS's and FBI's Fingerprint Systems**

Over the past several years, the OIG has examined the Justice Management Division's (JMD) efforts to integrate the INS's Automated Biometric Identification System (IDENT) and the FBI's Integrated Automated Fingerprint Identification System (IAFIS). In December 2001, we reported that the integration project was a year behind schedule. We also reported that the INS planned to implement several interim measures to enhance IDENT until it was integrated with IAFIS.

In June 2003, we issued a follow-up report that reviewed the progress made in integrating IDENT and IAFIS and found that the project continues to be delayed. When we issued our December 2001 report, the next major milestone for the integration project was the deployment of the initial integrated version of IDENT/IAFIS. At that time, deployment had been delayed from December 2001 to December 2002. Our June 2003 review found JMD had missed the December 2002 deployment date and now plans to deploy the initial integrated version in December 2003 – two years later than originally planned.

According to JMD officials, the deployment date has been delayed until December 2003 because the contractors and INS staff dedicated to the integration project were redirected in June 2002 to implement the National Security Entry-Exit Registration System (NSEERS). We found that despite the mounting delays, JMD did not prepare a revised schedule for completing the integration of IDENT and IAFIS. We also found that JMD did not develop a transition plan for continued management of the project once the INS transferred to the DHS in March 2003. Consequently, the integration project, already behind schedule, is likely to experience further delays.

The delays are significant because the interim enhancements to IDENT have shown the importance of integrating INS and FBI fingerprint information. Specifically, the INS and the FBI entered

into IDENT 152,200 National Crime Information Center "wants and warrants" fingerprint records on individuals who were likely to be aliens. As a result of entering these records, the INS matched approximately 4,820 fingerprints of apprehended individual aliens with the fingerprint records of suspects wanted for a variety of serious criminal offenses. The INS also added to IDENT 179,500 fingerprint records of aliens from countries subject to NSEERS registration, which resulted in 3,440 individual matches from September 2002 to mid-April 2003.

We made four recommendations to JMD to better manage the IDENT/IAFIS project and prevent further delays, and JMD concurred with our recommendations.

### **Audit of the September 11 Victim Compensation Fund**

The *Air Transportation Safety and Stabilization Act* (Act) established the September 11 Victim Compensation Fund of 2001 (Fund) to compensate individuals who were injured or relatives of individuals who were killed in the terrorist attacks of September 11. The Attorney General, acting through a special master, promulgated rules and procedures and administers the program. Funds totaling \$5.12 billion were requested for FYs 2002, 2003, and 2004 under a permanent and indefinite appropriation established by the Act.

Our audit concluded that Fund officials have developed rules and procedures in accordance with the Act, and awards are being processed in a consistent and timely manner. Adequate fraud controls were established to minimize the risks of fraudulent payments, and delays in processing appear largely attributable to the slow submission of documentation by the claimants. At the time of our audit, the requested funds appeared adequate to pay all of the awards. Fund officials stated they were preparing for an anticipated surge in the number of claims filed as the application deadline approaches, most likely by adding additional contract personnel and hearing officers.

### Follow-Up Audit of the Department's Counterterrorism Fund

The Department's Counterterrorism Fund (Fund) was established in 1995 to reimburse its components for the unanticipated costs of responding to and preventing terrorism. Although the initial legislation provided reimbursement only to Department components, since 1996 Congress has allowed over \$167 million to be passed through the FBI, JMD, and OJP to federal, state, and local users outside the Department. JMD, the administrative arm of the Department, administers the Fund and enters into reimbursement agreements with Department components to disburse the funds.

The OIG previously reviewed the Fund in a September 1999 report that covered Fund activities between FYs 1995 and 1997. We identified over \$4 million in dollar-related findings and concluded that JMD needed to strengthen its controls over the distribution and use of Fund monies, particularly funds passed through to non-Department users. As a result of the audit, \$4.3 million was returned to the Fund.

In this follow-up audit, the OIG reviewed activities for FYs 1998 through 2002. The OIG tested more than \$38 million in expenditures, including about \$36 million expended directly by Department components and over \$2 million passed through to other users.

The OIG again found weaknesses in the management and administration of the Fund and identified about \$3 million in dollar-related findings, including the following:

- ◆ The USMS did not adequately manage its reimbursements from the Fund. Specifically, the USMS improperly used or could not support almost \$1.3 million of the \$1.5 million we reviewed.
- ◆ Our testing at the FBI resulted in over \$1.3 million in questioned costs or 4 percent of the \$32.6 million reviewed. The FBI has shown progress since the prior audit when its error rate was 12 percent.
- ◆ In general, the funds passed through to users outside the Department continued to be at risk

because the Department components responsible for the funds did not adequately monitor the expenditures. As a result, about \$430,000 was improperly used or unsupported.

The OIG offered 13 recommendations to JMD for improving its administration of the Fund, including a recommendation that JMD increase its oversight of the components' management of Fund monies. JMD concurred with our recommendations.

### Department 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 oversees and issues the audits based on the work performed by independent public accountants. During this reporting period, we issued ten FY 2002 financial statement audit reports on Department components:

- ◆ Assets Forfeiture Fund and Seized Asset Deposit Fund
- ◆ Drug Enforcement Administration
- ◆ Federal Bureau of Investigation
- ◆ Federal Bureau of Prisons
- ◆ Federal Prison Industries, Inc.
- ◆ Immigration and Naturalization Service
- ◆ Offices, Boards and Divisions
- ◆ Office of Justice Programs
- ◆ U.S. Marshals Service
- ◆ Working Capital Fund

Each of these audits was in support of the FY 2002 consolidated Department of Justice audit, which was issued in the OIG's prior semiannual reporting period. For the second consecutive year, the Department received an unqualified opinion on its consolidated financial statement. Additionally, the number of material weaknesses reported at the consolidated level declined from three to two. These results reflect a continued commitment by the Department to financial accountability and improvement in internal controls.

The Department's unqualified opinion also included unqualified opinions on all ten of the reporting components' financial statements that make up the consolidated report. Importantly, some components were able to reduce the number of material weaknesses and reportable conditions. Overall, the material weaknesses reported at the various components declined from 13 to 9. In particular, the DEA eliminated the four material weaknesses reported in FY 2001.

While improvements in internal controls have been made, several material weaknesses remain in financial accounting and reporting procedures and in information systems. These weaknesses have been persistent over several years. They represent significant risks that data processed on the Department's information systems is not adequately protected from unauthorized access or service disruption and that the Department will not be able to meet the accelerated reporting requirements in future years.

As in prior years, issues related to financial accounting and reporting have only been overcome by significant year-end manual efforts. Many tasks had to be performed manually because the Department lacks automated systems to readily support ongoing accounting operations, financial statement preparation, and the audit process. Manual efforts compromise the ability of the Department to prepare financial statements that are timely and in accordance with generally accepted accounting principles, require considerable monetary and human resources, and represent an inefficient use of these resources. The manual processes are being strained further by the accelerated due dates and additional requirements established by the Office of Management and Budget (OMB). During FY 2003, quarterly financial statements were due 45 days after the close of the quarter, and for FY 2004, the *Performance and Accountability Report* is due by November 15, 2004, nearly 2½ months earlier than the current OMB reporting deadline.

Overall, nine of ten components had weaknesses in financial accounting and reporting. This finding primarily reflected problems in recording transactions in accordance with generally accepted accounting principles and meeting requirements of the Department's financial statement guide-

lines. Eight of ten components also had weaknesses in financial management systems' general and application controls. In the *Report on Compliance With Laws and Regulations*, the auditors also identified five Department components that were not compliant with the *Federal Financial Management Improvement Act of 1996*, which specifically addresses the adequacy of federal financial management systems. The auditors recommended that the Department revise the departmentwide financial statement reporting requirements and monitor components' compliance and efforts to correct all deficiencies noted. The Department concurred with the recommendations.

The following table compares the FY 2002 and 2001 audit results for the Department's consolidated audit as well as for the ten individual components' audits.

## Comparison of FY 2002 and FY 2001 Audit Results

Reporting Entity	Auditors' Opinion On Financial Statements		Number of Material Weaknesses		Number of Reportable Conditions	
	2002	2001	2002	2001	2002	2001
Consolidated Department of Justice	Unqualified	Unqualified	2	3	0	0
Assets Forfeiture Fund and Seized Asset Deposit Fund	Unqualified	Unqualified	0	0	1	0
Drug Enforcement Administration	Unqualified	Unqualified	0	4	2	1
Federal Bureau of Investigation	Unqualified	Unqualified	3	3	0	1
Federal Bureau of Prisons	Unqualified	Unqualified	0	0	2	0
Federal Prison Industries, Inc.	Unqualified	Unqualified	1	2	1	2
Immigration and Naturalization Service <sup>1</sup>	Unqualified	Unqualified	3	3	0	1
Offices, Boards and Divisions	Unqualified	Unqualified	1	0	1	2
Office of Justice Programs	Unqualified	Unqualified	0	0	1	3
U.S. Marshals Service	Unqualified	Unqualified	0	1	2	2
Working Capital Fund	Unqualified	Unqualified	1	0	0	0
Component Totals			9	13	10	12

<sup>1</sup> INS was audited through February 28, 2003.



### Department's Information Security Program and Practices

To assess the overall condition of the Department's IT security, the OIG evaluated broader themes and concerns extracted from ten IT security reports we issued in FYs 2001 and 2002 in response to the *Government Information Security Reform Act* (GISRA). In a consolidated report issued in FY 2003, we assessed the Department's IT security program as "fair," using a scale of excellent, good, fair, and poor, and concluded the program requires improvement at both the Department and component levels.

Our past GISRA audits have reported progress by the Department in improving aspects of its IT security program, particularly with the new chief information officer's initiatives that include plans to establish a central IT security office. Many deficiencies found in FY 2001 GISRA reviews, however, were found again in FY 2002. Our audit of the Department's classified and sensitive but unclassified systems revealed vulnerabilities in the management, operational, and technical controls that protect each system and its data from unauthorized use, loss, or modification. Of these three control areas, we concluded the vulnerabilities noted in technical controls were the most significant because those controls prevent unauthorized access to system resources by restricting, controlling, and monitoring system access.

Additionally, we found inconsistencies in the oversight of computer security, which we attributed to the bifurcation of responsibility between JMD's Security and Emergency Planning Staff and its Information Management and Security Staff offices. Reviews conducted by these two offices of the Department's IT systems were uneven or inadequate and major systems and applications lacked elementary protections that the Department's accreditation process was intended to ensure were in place. Our consolidated report made nine recommendations for improving management of computer security, and the Department concurred with our recommendations.

In FY 2003, we reviewed the Department's systems pursuant to the *Federal Information Security Management Act* (FISMA), which was enacted into law as Title III of the *E-Government Act of 2002*

(Public Law 107-347, December 17, 2002). FISMA replaced GISRA and contained stronger permanent provisions, including requirements for minimum mandatory information security standards.

FISMA directs the OIG to perform an annual independent evaluation of the Department's information security program and practices and requires the results to be submitted to the OMB. For FY 2003, we selected five mission-critical Department computer systems – two from the FBI and one each from the DEA, USMS, and ATF. Additionally, we are reviewing the Department's oversight initiatives with respect to computer security.

While we concluded that these components have made some progress in enhancing aspects of their computer security, continued improvements are needed in program oversight and vulnerability management. Of the five systems we reviewed, we assessed three systems as "high risk" and two systems as "medium risk" to protection from unauthorized use, loss, or modification. "High risk" is defined as presenting a strong need for corrective measures. "Medium risk" is defined as needing corrective actions and requiring a plan be developed to incorporate these actions within a reasonable period.

### COPS Grant Audits

We continue to audit grants awarded by COPS. During this reporting period, we issued 14 audit reports on the implementation of COPS hiring and redeployment grants. Our audits identified more than \$7.6 million in questioned costs and more than \$1.4 million in funds to better use. Examples of findings reported in our audits of COPS grants include the following:

- ◆ The Providence, Rhode Island, Police Department was awarded in excess of \$4.6 million in COPS grants to hire 14 additional law enforcement officers and to redeploy 148 police officers into community policing activities through the hiring of civilians and the purchase of equipment. We determined that the police department had not hired and properly retained all the civilians authorized and could not demonstrate redeployment of any of the 148 officer positions into community policing. As a result of these

deficiencies, we identified in excess of \$2.7 million in questioned costs and recommended \$887,645 be put to better use.

- ◆ The Asbury Park, New Jersey, Police Department was awarded in excess of \$3.1 million in COPS grants to hire 18 additional law enforcement officers and to redeploy 5 police officers into community policing activities through the hiring of civilians and the purchase of equipment. We determined that the police department charged unsupported costs to grant funds, could not support its local matching funds, had not hired all the civilians authorized, and could not demonstrate redeployment of any of the 5 officer positions into community policing. As a result of these deficiencies, we identified in excess of \$1.2 million in questioned costs and recommended \$238,181 be put to better use.
- ◆ The National City, California, Police Department was awarded in excess of \$1 million in COPS grants to hire 9 additional law enforcement officers and to redeploy 14 police officers into community policing activities through the purchase of technology. We determined that the police department received excess reimbursement and could not demonstrate redeployment of any of the 14 officer positions into community policing. As a result of these deficiencies, we identified \$358,744 in questioned costs.

### State and Local Equitable Sharing Audit

The Department's equitable sharing program exists to enhance cooperation among federal, state, and local law enforcement agencies by sharing federal forfeiture proceeds. State and local law enforcement agencies may receive equitable sharing revenues by participating directly with Department components in joint investigations leading to the seizure or forfeiture of property. The amount shared with the state and local law enforcement agencies is based on the degree of the agencies' direct participation in a case.

During this reporting period, we audited the Compton, California, Police Department's accountability and use of more than \$2.3 million in cash and proceeds received through the equitable sharing program during a 9-year period. We found that

the city of Compton and its police department were in material noncompliance with Department of Justice guidelines governing the accountability and use of equitable shared forfeited assets. For example, the city of Compton improperly transferred in excess of \$1.4 million from the equitable sharing fund account to the city's general fund account, and more than \$1.9 million reportedly used for police department salary expenditures was not supported by documentation. As a result, we questioned in excess of \$2.1 million in equitable sharing funds – all of the revenues received and interest earned by the Compton Police Department through 2000.

In September 2000, the Compton Police Department was dissolved, and the Los Angeles County Sheriff's Department took over the policing responsibilities in Compton. We found the sheriff's department to be in general compliance with Department of Justice guidelines and did not question any equitable sharing funds awarded to the sheriff's department.

### Superfund Audit for FYs 2000 and 2001

The *Comprehensive Environmental Response, Compensation, and Liability Act of 1980* (known as Superfund) provides for liability, compensation, cleanup, and emergency response for hazardous substances released into the environment and for uncontrolled and abandoned hazardous waste sites. The Department conducts and controls all litigation arising under Superfund and is reimbursed through interagency agreements with the Environmental Protection Agency (EPA). These agreements authorize reimbursement to the Department's Environment and Natural Resources Division (ENRD) for direct and indirect litigation costs. The EPA authorized \$28.6 million and \$28.4 million under the agreements in FYs 2000 and 2001, respectively, and the ENRD contracted with an accounting firm to maintain a system of accounting controls for these funds.

Our audit compared reported costs on the contractor-developed Accounting Schedules and Summaries for FYs 2000 and 2001 to those recorded on the Department's accounting records and reviewed the cost distribution system used by the ENRD to allocate incurred costs to Superfund and non-Superfund cases. Based on the results of

the audit, in our judgment the ENRD provided an equitable distribution of total labor costs, other direct costs, and indirect costs to Superfund cases during FYs 2000 and 2001.

### Trustee Audits

The OIG conducted performance audits of trustees under a reimbursable agreement with the Executive Office for U.S. Trustees (EOUST). During this reporting period, we issued 110 reports on the Chapter 7 bankruptcy practices of private trustees under Title 11, United States Code (Bankruptcy Code).

The Chapter 7 trustees are appointed to collect, liquidate, and distribute personal and business cases under Chapter 7 of the Bankruptcy Code. As a representative of a bankruptcy estate, the Chapter 7 trustee serves as a fiduciary protecting the interests of all estate beneficiaries, including creditors and debtors.

Our audits found that some trustees were deficient in documenting monthly bank reconciliations of estate accounts, maintaining receipts logs, investing estate funds properly, depositing estate funds in a timely manner, developing disaster recovery plans for financial and administrative records, implementing computer security, separating cash handling and recording duties, and maintaining support and authorizations for receipts and disbursements.

The OIG will not enter into a reimbursable agreement with the EOUST to perform Chapter 7 trustee audits in FY 2004 and instead will conduct more OJP grant audits and program reviews.

### Single Audit Act

The *Single Audit Act of 1984*, as amended, requires recipients of more than \$300,000 in federal funds to arrange for audits of their activities. Federal agencies that award federal funds must review these audits to determine whether prompt and appropriate corrective action has been taken in response to audit findings. During this reporting period, the OIG reviewed and transmitted to OJP 93 reports encompassing 569 Department contracts, grants, and other agreements totaling more

than \$1 billion. These audits report on financial activities, compliance with applicable laws, and the adequacy of recipients' management controls over federal expenditures.

## Investigations

The following are some of the cases investigated by the OIG during this reporting period that involved multiple components of the Department:

- ◆ In the Southern District of Texas, a former Kandleton, Texas, police chief and a former police captain were arrested on charges of conspiracy, wire fraud, and interference with commerce. An investigation by the OIG's Houston Area Office, the FBI, and the Texas Department of Public Safety led to a 52-count indictment alleging that the officers conspired to make materially false statements to the COPS grant program and to defraud the government of grant money earmarked to hire new police officers. The officers allegedly falsely claimed that more than \$200,000 in grant funds received had been used to hire six new police officers but instead used some of the grant funds to pay the police chief's salary. The indictment further alleges that the officers conspired to operate an extortion scheme in which Kandleton police officers used speed traps to collect sums of money above those set by state law.
- ◆ In a dispute over the alleged mischarging of personnel costs on a Department Criminal Division contract, Logicon, Incorporated (Logicon) agreed to pay the Department \$175,000 and withdraw claims totaling an additional \$51,489 in a settlement reached in April 2003. The settlement arose out of an inquiry led by the OIG's Fraud Detection Office, which discovered questionable charges for personnel costs at a rate higher than appropriate based on Logicon employees' professional credentials. The OIG's Office of General Counsel worked closely with the Department's Civil Division Commercial Litigation Branch to achieve the recovery.
- ◆ A civilian was sentenced in the Western District of Arkansas to 18 months' incarceration after she pled guilty to charges of mail fraud for sub-

mitting a fraudulent application to the September 11 Victim Compensation Fund (Fund). An investigation by the Fraud Detection Office developed evidence that the civilian applied for benefits from the Fund claiming that her brother, a New York City fireman, was killed in the terrorist attacks. In fact, the civilian did not have a brother who was a New York City fireman killed in the terrorist attacks.

- ◆ At the request of the Office of the Attorney General, the OIG investigated allegations that the INS provided misleading reports to the Attorney General on whether certain countries should remain participants in the Visa Waiver Program. The program allows nationals of countries designated by the Attorney General to enter the United States temporarily without first securing a nonimmigrant visa from a United States Consulate overseas. The *Immigration and Naturalization Act* requires the Attorney General, in consultation with the Secretary of State, to determine periodically whether to continue or terminate countries in the program. Beginning in late 2001, the former INS initiated an interagency review of the designation of six program countries. In September 2002, the INS forwarded to the Attorney General reports evaluating the effect of the continued designation of these countries on the United States' interests, including the federal government's interest in enforcement of the immigration and general criminal laws and national security. Based on those evaluations, the reports recommended either the continued designation or termination of each country under review. Shortly after the INS forwarded the reports to the Attorney General, an INS official alleged that other INS officials edited drafts of the reports to omit or mischaracterize significant information. Our investigation found insufficient evidence to support the allegation that INS officials improperly edited the reports to omit or mischaracterize relevant information regarding the risks posed by the continued designation of the countries under review.

## Ongoing Work

### Protection of Critical Cyber-Based Infrastructure

The Department and other government departments and agencies are required to prepare and implement plans for protecting critical infrastructure. The infrastructure includes systems essential to the minimum operations of the economy and government, such as telecommunications, banking and finance, energy, and transportation. In this ongoing audit, we are focusing on the adequacy of the Department's implementation activities for protecting critical computer-based infrastructure. Specifically, we are reviewing activities in the areas of risk mitigation, emergency management, interagency coordination, resource and organization requirements, the recruitment and education of IT personnel, and computer security awareness.

### Collection and Dissemination of Arson and Explosives Intelligence

The OIG is conducting an audit of the FBI's Bomb Data Center and the ATF's Arson and Explosives Information System. Our objective is to determine how the Department can most efficiently and effectively collect – and make available to the law enforcement community – information on arson and criminal misuse of explosives.

### Department Acquisition Processes

The Department is one of the federal agencies with the largest dollar expenditures for the acquisition of products and services, averaging approximately \$4 billion a year in contracts. JMD has oversight responsibilities for acquisitions by Department components. This audit is evaluating the acquisition processes used by the bureaus and JMD's oversight of acquisitions. The focus of the audit is to assess whether needed products are acquired in a timely manner for an economical price within governing regulations.

**The Department's Counterterrorism Task Forces**

The OIG is examining how the Department's counterterrorism task forces support the Department's efforts to detect, deter, and disrupt terrorism. The review is specifically evaluating the purpose, priorities, membership, functions, lines of authority, and accomplishments for the USAOs' Anti-Terrorism Task Forces, the FBI's Joint Terrorism Task Forces and Foreign Terrorist Tracking Task Force, and the Deputy Attorney General's National Security Coordination Council.

**OJP's Technical Assistance and Training Grants**

This audit is evaluating OJP's methods for approving technical assistance and training grants and assessing the management, quality, and extent of the technical assistance and training provided.



# The Federal Bureau of Investigation

The FBI is the principal investigative arm of the Department. Its investigative jurisdiction encompasses more than 200 federal laws, including civil rights, counterterrorism, foreign counterintelligence, organized crime, violent crime, and financial crime. FBI headquarters in Washington, D.C., coordinates the activities of 56 field offices, approximately 400 satellite offices, and more than 40 foreign liaison posts that work abroad on criminal matters within the FBI's jurisdiction. The FBI has approximately 27,000 employees: 11,000 special agents and more than 16,000 professional support personnel.

## Reports Issued

### **The FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen**

Over the course of more than 20 years, former FBI supervisory special agent Robert Philip Hanssen compromised some of this nation's most important counterintelligence and military secrets, including the identities of dozens of human sources, at least three of whom were executed. Hanssen's espionage began in November 1979 – three years after he joined the FBI – and continued intermittently until his arrest in February 2001, just two months before his mandatory retirement date.

Shortly after his arrest, the Senate Select Committee on Intelligence and the Attorney General asked the OIG to review the FBI's performance in connection with the Hanssen case. In response, the OIG analyzed more than 368,000 pages of material and conducted more than 200 interviews and in August 2003 completed a 674-page report describing the results of the review.

This report is classified at the Top Secret/Codeword level because it contains extremely sensitive classified information regarding sources involved in the case and FBI counterintelligence activities. The OIG also produced a 383-page version of the report classified at the Secret level and a 31-page unclassified executive summary to provide a public summary of the main findings.

Our review of the Hanssen case revealed that there was little deterrence to espionage at the FBI during Hanssen's 25-year career. The FBI did not employ basic personnel security techniques – such as counterintelligence polygraph examinations and financial disclosure reviews – and the one background reinvestigation Hanssen underwent during his career was not thorough. In addition, Hanssen was not closely supervised for most of his FBI career. He committed flagrant security breaches and indiscretions, many of which came to the attention of coworkers and supervisors. Only one of Hanssen's security violations was documented, and he was never disciplined for any of his misconduct.

The FBI's information security program likewise offered little deterrence to Hanssen's espionage. Because of inadequate document security, Hanssen felt comfortable removing hundreds of pages of classified documents from FBI offices, including numbered original Top Secret documents. And because of inadequate computer security, Hanssen felt free to conduct thousands of searches on the FBI's computer system for references to his own name, address, and drop and signal sites to see if he was under suspicion and to search for information concerning the FBI's most sensitive counterintelligence cases. The computer system's audit function, mandated by Department regulation and a principal tool against unauthorized use as well as espionage, was rarely used before Hanssen's arrest.

In addition to its management responsibility to detect espionage among its employees, the FBI is the lead agency for detecting and investigating espionage committed in the United States. Our review of the Hanssen case found that the FBI's efforts against penetration in the late 1970s and 1980s suffered from a lack of cooperation between the FBI and the Central Intelligence Agency (CIA) and from inattention and indifference regarding serious intelligence losses. Although the FBI pursued several penetration investigations between 1993 and 2000, Hanssen received no investigative scrutiny until late 2000. Until the FBI identified Hanssen, it never opened even a preliminary inquiry on any FBI employee in connection with the search for a mole, even though a mole – ultimately identified as Hanssen – was believed to have compromised a large number of FBI assets and operations.

In sum, the OIG found that Hanssen escaped detection not because he was extraordinarily clever and crafty, but because of long-standing systemic problems in the FBI's counterintelligence program and a deeply flawed internal security program. Over the years, the FBI demonstrated an institutional reluctance to consider itself as a possible source for a penetration in the absence of information identifying a specific FBI target. The FBI's reluctance to recognize the possibility that an FBI employee might commit espionage also was reflected in the FBI's failure to implement an effective internal security program, particularly after the 1994 arrest of CIA officer Aldrich Ames for espionage. Ineffective oversight by FBI management and poor coordination with the Department contributed to the FBI's failure to pursue appropriate avenues of investigation.

The OIG's report made 21 recommendations to help the FBI improve its internal security and enhance its ability to deter and detect espionage in its midst. For example, the OIG recommended that the FBI create a new unit at FBI headquarters dedicated to determining whether the FBI has been penetrated. The OIG also recommended that the FBI create a senior operational position in the Counterespionage Section at FBI headquarters to be filled, on a rotating basis, by senior executives from the CIA and other components of the intelligence community. In addition, the OIG made recommendations for enhancing coordination with

the Department and for improving personnel, document, and computer security.

### **Implementation of Information Technology Recommendations**

As computer technology has advanced, federal agencies have become increasingly dependent on information systems to carry out operations and to process, maintain, and report essential information. The FBI's computerized information systems affect many of its mission-critical activities, such as financial management, security of sensitive and classified data, and investigative work.

Recognizing the importance and vulnerability of data processed, maintained, and reported by the FBI, the OIG has conducted various audits and reviews of the FBI's management of IT. Since 1990, reports issued by the OIG have found numerous deficiencies with the FBI's IT program, including outdated infrastructures, fragmented management, ineffective systems, and inadequate training.

The audit we issued in September 2003 assessed the FBI's implementation of IT recommendations in previous OIG reports. While the FBI had implemented many of the recommendations (93 out of 148), significant further actions are necessary to ensure that the IT program effectively supports the FBI's mission. For example, recent audits and reviews conducted by the OIG have found repeated deficiencies with the FBI's IT control environment and compliance with information security requirements.

These repeated deficiencies indicate that, in the past, FBI management had not paid sufficient attention to improving the agency's IT program. Until recently, the FBI lacked an effective system of management controls to ensure that the OIG's recommendations are implemented in a timely and consistent manner. However, current leadership has stated that the FBI is committed to enhancing controls to ensure recommendations were implemented in a consistent and timely manner. The FBI has recently established a system to facilitate the tracking and implementation of recommendations. Additionally, the FBI expects significant improvements from its IT modernization efforts, which it believes will correct many of the deficien-

cies identified by the OIG. Our report offered three recommendations, with which the FBI agreed, to improve the FBI's tracking, resolution, and implementation of IT recommendations.

### Casework and Human Resource Allocation

In its 1998 strategic plan, the FBI identified foreign intelligence, terrorist, and criminal activities that directly threaten the national security of the United States as its top priority. This OIG audit of the FBI's casework and human resource allocation, issued in September 2003, analyzed trends in the resources used to investigate the various categories of crimes under the FBI's jurisdiction and the types and numbers of cases investigated. We found that prior to the September 11, 2001, terrorist attacks, the FBI devoted significantly more special agent resources to traditional law enforcement activities – such as investigating white collar crime, organized crime, drugs, and violent crime – than it did to terrorism-related programs. The audit also revealed:

- ◆ The terrorism-related programs consistently underutilized their allocated personnel resources at a rate greater than the FBI as a whole. In comparison, agent utilization rates in the Violent Crime and Major Offenders, Civil Rights, and White Collar Crime programs were significantly higher.
- ◆ Only 4 of the 56 field offices expended more of their agent resources in a terrorism-related program than in any other program. The remaining 52 field offices predominantly used agent resources in the White Collar Crime, Violent Crime and Major Offenders, or Organized Crime/Drugs programs.
- ◆ Terrorism-related cases accounted for only 18 percent of those open any time between October 1995 and June 2002. In contrast, the Violent Crime and Major Offenders program accounted for 25 percent of this universe of cases.

The FBI responded to the September 11 attacks with a level of effort unprecedented in its history. In a comparatively short time, the investigation into the attacks became the FBI's largest major case in the past seven years. Additionally, since September 11, the FBI has continued to devote

more of its time to terrorism-related work than to any other single area.

The OIG provided seven recommendations to help the FBI create an environment in which its operational priorities, in terms of human resources and investigations, consistently coincide with the priorities that it has identified in its strategic plan. Specifically, the OIG recommended that the FBI (1) regularly review resource allocation reports for the FBI as a whole, as well as for the individual investigative programs, and explore additional means of analyzing the FBI's resource use among the various programs; (2) research and implement methods for addressing the overutilization and high allocation of agent resources in the Violent Crime and Major Offenders program; and (3) review its current planning factors and processes to more closely approximate the agent resources the FBI actually needs. The FBI generally agreed with our recommendations.

## Investigations

During this reporting period, the OIG received 435 complaints involving the FBI. The most common allegations made against FBI employees included job performance failure, waste and misuse of government property, and improper release of information. The OIG investigated many of the most serious allegations and referred others to the FBI Office of Professional Responsibility (OPR).

At the close of the reporting period, the OIG had 61 open cases of alleged misconduct against FBI employees. The criminal investigations cover a wide range of offenses, including the improper release of law enforcement information and theft of government property. The administrative investigations include serious allegations of misconduct, including allegations against high-level employees. The following are some of the cases investigated during this reporting period.

- ◆ An FBI language specialist assigned to the El Paso Field Division was arrested in the Western District of Texas on charges of unauthorized access of a computer for financial gain, making false statements, and trafficking in and using fraudulently obtained cellular



phones. An investigation by the OIG's El Paso Area Office, the FBI, the Internal Revenue Service, and the El Paso County Sheriff's Office led to three separate indictments alleging that the language specialist intentionally accessed an FBI computer on six occasions for the purpose of private financial gain, made false statements to federal agents, and collected more than \$1,000 in money from trafficking in and using fraudulently obtained cellular telephones. Losses to the cellular telephone company are estimated at \$137,000. The language specialist pled guilty and was sentenced to five years' incarceration and three years' supervised release.

- ◆ The OIG received allegations that an FBI special agent disclosed sensitive law enforcement information relating to an FBI investigation to a subject with whom the agent was having an intimate relationship and from whom the agent was receiving gifts, including money and two vehicles. In the course of the joint OIG Boston Area Office and FBI OPR investigation, the special agent admitted to having a 4-year affair and accepting approximately \$50,000 in gifts from a woman who the agent knew to be a subject of a criminal probe. The agent further admitted to discussing the investigation with her. The Public Integrity Section declined criminal prosecution of this case. The OIG has recommended the agent's termination from the FBI.
- ◆ The OIG investigated allegations that an FBI certified forensic examiner committed perjury during testimony at a hearing in a murder case in Lexington, Kentucky. The investigation was prompted when the examiner admitted to the FBI Laboratory chief that, during the hearing, the examiner had misrepresented the date that a bullet manufacturer began receiving its lead in billet (previously melted and shaped) form. The OIG investigation established that the examiner had knowingly given erroneous testimony at the hearing. In June 2003, the examiner pled guilty in Kentucky state court to a misdemeanor charge of false swearing. The examiner received a sentence of 90 days' imprisonment, which was "conditionally discharged" upon successful completion of a probationary period, and a \$250 fine.
- ◆ In our March 2003 *Semiannual Report to Congress*, we reported that two FBI special agents assigned to the San Antonio Division had surreptitiously recorded the conversations of an FBI assistant special agent in charge and a supervisory special agent. The OIG's El Paso Area Office investigation concluded that the first FBI special agent lied to and deceived a fellow FBI employee, was not forthcoming with FBI OPR and OIG investigators, and misused FBI electronic intercept equipment in a personal dispute with FBI management. Regarding the allegations against the second special agent, the OIG found that he lied to FBI OPR and OIG agents in three separate affidavits when he denied participating in the surreptitious recording of FBI managers. During this reporting period, the second special agent pled guilty to a charge of lying to federal investigators and was sentenced to one year of supervised probation. He resigned from the FBI as a result of this investigation.
- ◆ In our March 2003 *Semiannual Report to Congress*, we reported that an FBI crime scene photographer in the Baltimore FBI office was arrested and pled guilty in the District of Maryland to charges of theft of government property. A joint investigation by the OIG's Washington Field Office and the FBI revealed that between 1999 and 2002, the photographer stole at least \$83,000 worth of photography supplies and equipment from the FBI and sold them over the Internet. During this reporting period, the photographer was sentenced to one year of incarceration and three years' supervised release and was ordered to pay \$70,000 in restitution.

## Ongoing Work

### The FBI's Handling of Intelligence Information Prior to the September 11 Attacks

At the FBI director's request, the OIG is reviewing issues related to the FBI's handling of intelligence information prior to the September 11, 2001, terrorist attacks. The investigation is focusing on how the FBI handled an electronic communication written by its Phoenix Division in July 2001

regarding extremists attending civil aviation schools in Arizona, the FBI's handling of the Zacarias Moussaoui investigation, and other issues concerning the FBI's handling of information or intelligence before September 11 that might relate to the terrorist attacks.

### **DNA Laboratory**

The OIG is reviewing the failure of a former technician in the FBI Laboratory DNA Analysis Unit to complete steps designed to detect contamination in the analysis process. In addition, with the assistance of nationally known DNA scientists, the OIG is conducting a broader assessment of the DNA Analysis Unit's protocols and procedures to determine if other vulnerabilities exist in its operations.

### **The Legal Attaché Program**

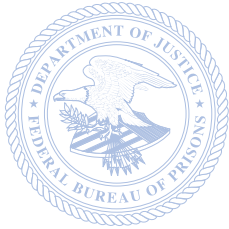
The Legal Attaché program was created to establish greater cooperation with international police partners in support of the FBI's mission. The FBI has legal attaché offices in 46 countries. The OIG is auditing the effectiveness of the legal attaché offices in establishing liaisons with foreign law enforcement agencies, the criteria and process used by the FBI to determine the location of offices and the oversight and management of existing offices, and the types of activities attachés perform and whether they overlap with other federal enforcement agencies' activities.

### **Efforts to Improve the Sharing of Intelligence and Other Information**

The OIG is conducting an audit of the FBI's progress in addressing deficiencies in its intelligence-sharing capabilities identified by the FBI, Congress and the OIG. The primary objectives of the audit are to determine the extent to which the FBI has identified impediments to the sharing of counterterrorism intelligence and other information, has improved its ability to share intelligence and other information both internally and with the intelligence community and with state and local law enforcement agencies, and is providing useful threat and intelligence information to intelligence and law enforcement agencies.

### **Language Translation Services**

The OIG is conducting an audit of the FBI's language translation services program. The audit's objectives are to determine the extent and causes of any FBI translation backlog; assess the FBI's efforts to hire additional translators; and evaluate whether FBI procedures ensure appropriate prioritization of work, accurate and timely translations of pertinent information, and proper security of sensitive information.



# The Federal Bureau of Prisons

The BOP operates a nationwide system of prisons and detention facilities to incarcerate and detain inmates who have been imprisoned for federal crimes or who are awaiting trial or sentencing in federal court. The BOP consists of approximately 33,900 employees, 103 institutions, 6 regional offices, 2 staff training centers, and 29 community corrections offices. The BOP is responsible for the custody and care of approximately 171,500 federal offenders, 145,300 of whom are confined in BOP-operated correctional institutions and detention centers. The remainder are confined in detention centers, privately operated prisons, community corrections centers, juvenile facilities, and facilities operated by state or local governments.

## Reports Issued

### Procurement Activities for Prison Space in California City, California

The BOP is addressing its expanding population of federal offenders partly by obtaining housing for lower-security inmates through contracting with private contractors who own and operate low-security facilities. Currently, the BOP has seven contracts for low-security private prison space. Our audit focused on the procurement process the BOP used to acquire space from the Corrections Corporation of America (the contractor) facility in California City, California. This low-security facility has a capacity of 2,304 inmates. The BOP contract was for the exclusive use of the facility. The total amount of the contract for a 10-year period was estimated to be \$529 million.

Our audit assessed the cost-effectiveness of the procurement, the BOP award process, and the methodology used to identify prison space requirements. We also reviewed the financial condition of the contractor and the BOP's monitoring

of the contract and contractor subsequent to award.

We found that the BOP paid \$18.9 million for prisoner bed space that was not used during the first nine months of the contract because a procurement provision guaranteed the contractor payment for at least 95 percent of the stated capacity of the facility upon activation. The BOP may recover this amount paid over the life of the contract with the exercise of the contract option years. However, this recovery is predicated on the BOP's future need for this prison space at the current level and the contractor's ability to provide it.

Additionally, we determined that the BOP failed to obtain sufficient current financial information from the contractor and to adequately verify the contractor's ability to obtain the necessary financial resources prior to awarding the contract. As a result, the BOP did not have assurance that the contractor was financially viable at the time the award was made. We also found that the BOP's Acquisitions Branch constrained the final pre-award review of the contract by limiting the review period and by providing incomplete documentation. As a result, the BOP could not perform a detailed review to ensure compliance with established BOP policies or to ascertain the contractor's financial condition at that time. The BOP also failed to document all significant actions and events in the award process and the monitoring of the financial condition of the contractor subsequent to the award.

We made five recommendations for corrective action that included requiring the BOP to determine the benefit of payment guarantees in future procurements for prison bed space, reminding procurement officials of the importance of obtaining sufficient financial information from prospective contractors prior to awarding contracts, ensuring all procurements are adequately reviewed for

compliance with acquisition regulations, requiring procurement officials to document adequately all significant actions and decisions, and ensuring monitoring of the financial condition of contractors when significant weaknesses are identified. Although it disputed some of the findings, the BOP agreed with our recommendations and took corrective action necessary to address them.

### SENTRY Database

SENTRY, the BOP's primary mission support database, processes over 1 million transactions each day and tracks more than 171,500 federal inmates. The system collects, maintains, and tracks critical information, including inmate location, medical history, behavior history, and release data. To determine whether SENTRY data are valid, properly authorized, and completely and accurately processed, we assessed the system's application controls.

Using the criteria in the *Federal Information System Controls Audit Manual (FISCAM)*, we reviewed the accuracy and timeliness of SENTRY's input, processing, and output controls and conducted on-site reviews of the operational workflows at 3 of the BOP's 29 community corrections offices (Annapolis Junction, Maryland; Philadelphia, Pennsylvania; and Chicago, Illinois). These sites were selected because they process large volumes of inmate data into SENTRY.

Our audit identified weaknesses in 4 of the 27 FISCAM control areas that we tested: supervisory reviews, audit logs, access controls, and computer matching of transaction data. Specifically, we identified data input errors resulting in incorrect inmate offense/charge codes, incorrect inmate commitment dates, incorrect dates of offense, and missing offense fines. We also found that the BOP did not adequately monitor audit log exception reports. Our review of SENTRY's access controls disclosed that users with limited access profiles were able to process transactions above their level of access when logged onto terminals designated for users with higher authorization.

We concluded that these weaknesses occurred because BOP management did not fully develop, document, or enforce BOP policies in accordance with current Department policies and procedures.

Although we do not consider our findings to be major weaknesses, if not corrected they could impair the BOP's ability to ensure the integrity, confidentiality, and availability of the data in SENTRY.

We recommended that the BOP ensure that (1) its inmate data entry form is updated to reflect current procedures and needs, (2) its SENTRY System Security Guide requires the routine generation and review of exception reports, (3) timely exception reports are provided to the Information Security Officer, and (4) SENTRY's workstation controls are properly configured to allow access only to authorized areas of the system. The BOP agreed with our recommendations.

## Investigations

During this reporting period, the OIG received 2,628 complaints involving the BOP. The most common allegations made against BOP employees included job performance failure, use of unnecessary force, official misconduct, and security failure. The vast majority of complaints dealt with noncriminal issues that the OIG referred to the BOP Office of Internal Affairs.

At the close of the reporting period, the OIG had 271 open cases of alleged misconduct against BOP employees. The criminal investigations cover a wide range of allegations, including bribery of a public official, sexual abuse of inmates, and introduction of contraband (e.g., drugs). The following are some of the cases investigated during this reporting period.

- ◆ The OIG's San Francisco Area Office investigated allegations that a BOP senior correctional officer assigned to the Federal Correctional Institution (FCI) in Englewood, Colorado, verbally abused a Muslim inmate with derogatory racial, ethnic, and religious slurs. A BOP correctional officer and six inmates provided corroboration for the allegations. The subject subsequently provided a sworn statement admitting to making derogatory racial, ethnic, and religious slurs and to providing a "less than completely candid" memorandum concerning these incidents to a BOP investigator. This case was declined for prosecution by

the Civil Rights Division but was provided to the BOP for administrative action.

- ◆ A BOP captain at the U.S. Penitentiary (USP) in Atlanta, Georgia, was sentenced to 18 months' incarceration on charges of witness tampering and making false statements. A joint investigation by the OIG's Atlanta Area Office and the FBI determined that the BOP captain provided a false statement to investigators by denying he had a conversation with a former USP Atlanta case manager in which he informed the case manager that the OIG was investigating him. In addition, the BOP captain advised the case manager not to divulge the name of the person who tipped him off about the OIG investigation.
- ◆ A BOP correctional counselor assigned to the USP in Leavenworth, Kansas, was sentenced in the District of Kansas to 57 months' incarceration and 2 years' supervised release on charges of introducing contraband into the USP. A joint investigation by the OIG's Detroit Area Office and the FBI determined that the correctional counselor was attempting to smuggle marijuana and crack cocaine into the USP for an inmate. During an undercover operation, the correctional counselor accepted \$5,000 from an undercover Kansas City police officer to smuggle the narcotics into the USP.
- ◆ A former BOP physician was arrested pursuant to an indictment returned in the Northern District of Texas for sexual abuse of a ward. An investigation by the El Paso Area Office determined that the physician at the Federal Medical Center Carswell engaged in sexual intercourse with three female inmate patients on numerous occasions, primarily in his medical office. In addition, the physician admitted to engaging in sexual intercourse with a female employee in various locations within the medical center.
- ◆ A former BOP correctional officer was arrested and pled guilty in the Eastern District of Kentucky to making a false statement to obtain federal workers' compensation. A joint investigation by the OIG's Atlanta Area Office and the Department of Labor established that the former correctional officer falsely claimed that he was unable to work as a result of an on-the-job injury that occurred when he was employed at

the FCI in Manchester, Kentucky. The investigation disclosed that the correctional officer wrongfully collected in excess of \$100,000 in compensation during a time when he owned and operated a number of businesses, including a convenience store, a boat-hauling company, and an excavating company.

## Ongoing Work

### The BOP's Process for Selecting Muslim Clerics

The OIG is reviewing the procedures used by the BOP to select Muslim personnel, contractors, and volunteers who provide religious services to inmates. We initiated this review in response to a letter from a U.S. Senator expressing concerns that the BOP relies solely on two organizations that allegedly have connections to terrorism to endorse Muslim cleric candidates as qualified religious leaders. The OIG's review is examining whether the BOP's process effectively screens candidates to ensure that extremist groups do not become religious service providers in the BOP.

### Inmate Release Preparation and Transitional Reentry Programs

The OIG is auditing the BOP's Inmate Release Preparation and Transitional Reentry Programs to evaluate whether the BOP ensures that (1) its programs designed to prepare inmates for reentry into society – including educational, occupational, psychology services, and other programs – provide consistent quality of services among institutions and (2) eligible inmates are provided the opportunity to transition through a Community Corrections Center in preparation for reentry into society.

## 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 is an example of a PRR sent to the BOP during this reporting period.

- ◆ The OIG's Investigations Division prepared a PRR concerning the control and security of dental offices and clinics within BOP facilities. The PRR was the result of an investigation into allegations of bribery and theft of government property at the Three Rivers, Texas, FCI. The investigation determined that two inmate dental assistants established an illegitimate business within the FCI providing dental services to inmates for a fee, using BOP supplies and facilities. Although the investigation determined that the chief dental officer was not involved in the inmates' scheme, the freedom and responsibility the chief dental officer afforded the inmates far exceeded that prescribed by BOP policy. The investigation also determined that no inventories were conducted or supply records kept that would alert officials to the possible theft of dental supplies or materials. The OIG recommended that the BOP review its policy concerning the security of dental clinic operations and issue specific guidance for (1) monitoring the activities of inmates assigned to dental clinics, (2) performing regular inventories of dental supplies and equipment, (3) performing periodic searches of inmates and inspections of inmate work areas to ensure items are not removed from the clinic and that inmates are not performing unauthorized work, and (4) providing recurring training for BOP personnel on the need to monitor inmates under their supervision.



# The Drug Enforcement Administration

The DEA enforces laws and regulations of the United States related to the growing, manufacture, or distribution of controlled substances. In addition, the DEA recommends and supports programs aimed at reducing the availability of illicit controlled substances on the domestic and international markets. In FY 2003, the DEA had approximately 9,600 employees, almost half of whom were special agents. The DEA has 21 division offices in the United States and the Caribbean and maintains 79 offices in 58 countries throughout the world.

## Report Issued

### Implementation of the Government Performance and Results Act

Congress has mandated performance-based management in federal agencies through a series of statutory reforms, the centerpiece of which is GPRA. GPRA seeks to improve the effectiveness, efficiency, and accountability of federal programs by establishing a system for agencies to set goals for program performance and to measure results. Under GPRA, agencies must develop strategic plans that identify their long-range strategic goals and objectives, annual performance plans that set forth corresponding annual goals and indicators of performance, and annual performance reports that describe the actual levels of performance achieved compared with the annual goals.

This audit evaluated the DEA's implementation of GPRA. We examined whether the DEA had (1) developed an adequate strategic goal and objectives that were consistent with the Department's strategic goals and objectives; (2) established performance indicators for all decision units included in the DEA's budget requests; and (3) established an effective system

of controls to collect, analyze, and report performance data.

Our audit determined that the DEA had failed to meet key aspects of GPRA. We found that the DEA's strategic goal and objectives were not definitive enough to allow for an assessment of whether the goal and objectives were being achieved. In addition, even though the DEA had established performance indicators for all of its budget decision units, it had not established:

- ◆ Specific criteria for its field divisions to designate organizations as "priority target" organizations, which is a key element of its strategic goal;
- ◆ Specific criteria for its field divisions to report on the primary performance indicator – that is, priority target organizations disrupted or dismantled;
- ◆ An effective system to collect, analyze, and report performance data for all of its indicators;
- ◆ Procedures to verify the performance data for all of its indicators;
- ◆ Accurate performance data for one of the five field divisions included in our audit; and
- ◆ Realistic performance goals for its performance indicators.

As a result of these deficiencies, the ability of the DEA, the Department, Congress, and the public to assess the effectiveness of the DEA's performance is diminished. We recommended, among other things, that the DEA establish (1) a strategic goal and objectives that are quantitative, directly measurable, or assessment-based and (2) specific criteria for determining what constitutes a priority target organization and a disrupted or dismantled priority target organization. The DEA concurred with our recommendations and is updating its

strategic plan. The new strategic plan will include, according to the DEA, one general long-term goal and four strategic goals with quantitative, time-specific objectives that will address some of the OIG's recommendations.

## Investigations

During this reporting period, the OIG received 265 complaints involving the DEA. The most common allegations made against DEA employees included misuse of a credit card, job performance failure, and false statements. The OIG investigated many of the most serious allegations and referred others to the DEA OPR.

At the close of the reporting period, the OIG had 19 open cases of alleged misconduct against DEA employees. The following is an example of a case investigated during this reporting period.

- ◆ The OIG received allegations that a DEA special agent assigned to the Baltimore District Office engaged in an improper association with a known criminal. A joint OIG Washington Field Office and DEA OPR investigation found that the special agent had engaged in an improper association with a convicted felon serving a life sentence and had exercised poor judgment in this association. The agent acknowledged that he had (1) written personal letters to the inmate, (2) engaged in numerous personal telephone conversations with the inmate while on duty at the DEA office, (3) deposited personal funds into the inmate's commissary account, (4) met with the inmate alone, and (5) given the appearance that he had entered into a business transaction with the inmate. Additionally, the special agent acknowledged that these actions violated four provisions of the DEA Standards of Conduct. The OIG reported its findings to the DEA for appropriate administrative action.

## Ongoing Work

### Use of Informants

The DEA uses confidential sources (informants) as an investigative tool in support of criminal investi-

gations and the prosecution of drug cases. The OIG is assessing the DEA's payments to informants, compliance with regulations and controls over disbursements, and the effect that the information provided by informants has had on arrests and prosecution of cases.

### Discipline Process

The OIG is evaluating the process by which the DEA identifies, refers, and investigates employee misconduct and imposes discipline in response to substantiated allegations of employee misconduct.

### Control of Seized Narcotics and Cash

The OIG is assessing the policies, procedures, and practices used by DEA offices to control and safeguard the chain of custody for narcotics and cash evidence seized during DEA-controlled investigations or submitted into the DEA's custody as the result of seizures by other federal, state, and local law enforcement agencies. A review of the DEA's custodial accountability for evidence, initiated by the DEA administrator in 2000, resulted in the approval of recommendations to improve identified weaknesses in the DEA's evidence program. We are examining the DEA's progress in implementing those recommendations.

### Follow-Up Audit of the DEA's Laboratory Operations

The OIG is following up on our 1995 audit of the quality of the DEA's forensic laboratory operations. We are determining whether laboratory policies and procedures ensure that forensic examinations meet standards that support timely and appropriate case progress and disposition and whether laboratories properly account for evidence and other controlled substances. We also are evaluating customer satisfaction with laboratory services and whether any cases have been compromised because of any weaknesses in laboratory work.



# Other Department Components

## U.S. Marshals Service

The USMS is responsible for protecting the federal judiciary, transporting federal prisoners, protecting endangered federal witnesses, managing assets seized from criminal enterprises, and pursuing and arresting federal fugitives. The director and deputy director of the USMS work with 94 U.S. marshals, each appointed by the President and confirmed by the Senate, to direct the activities of 95 district offices and approximately 4,000 staff stationed at more than 350 locations throughout the 50 states, Guam, the Northern Mariana Islands, Puerto Rico, and the U.S. Virgin Islands.

## Investigations

The following is one of the cases investigated during this reporting period that involved the USMS:

- ◆ A deputy U.S. marshal assigned to the USMS's District of New Jersey's Asset Forfeiture Unit and his brother were convicted in the District of New Jersey on charges of conspiracy to defraud the United States, false statements, embezzlement, and mail fraud. An investigation by the New York Field Office developed information that the deputy U.S. marshal, while serving as the chief of the Asset Forfeiture Unit, disposed of forfeited vehicles and real estate in violation of USMS policy by selling them at a reduced price to family members and friends for cash.

## Ongoing Work

### Prisoner Medical Care

The USMS is responsible for providing medical care to the roughly 40,000 prisoners it has in its custody at any given time. The objectives of this audit are to determine whether (1) the USMS is providing prisoners necessary health care, (2) the USMS is screening and treating prisoners for communicable diseases, (3) prisoner medical costs are necessary and reasonable, and (4) the USMS is providing prisoners secure transport to off-site facilities to receive medical treatment.

### Budget Execution During FYs 2002 and 2003

The primary purpose of the audit is to determine whether the USMS executed its appropriated budgets for FYs 2002 and 2003 in accordance with congressional instructions.

### Administration of the Witness Security Program

The OIG is reviewing the USMS's administration of the Witness Security Program to evaluate plans and strategies for achieving the program's stated security objectives, controls for witness safety, and controls for financial activities, including payments to protected witnesses and their families.

### The Judicial Security Program

The OIG is assessing the USMS's actions since September 11, 2001, to improve its Judicial Security Program. This review focuses primarily on the USMS's efforts to identify, assess, and mitigate threats and terrorism risks against members of the federal judiciary.

## 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 11,500 employees work in those offices and in the Executive Office for U.S. Attorneys (EOUSA).

### Ongoing Work

#### Critical Incident Response Plans

To maximize the USAOs' ability to respond quickly and appropriately to critical incidents, the Attorney General directed each USAO to develop a critical incident response plan. This review is examining whether the plans have been developed and submitted to the EOUSA as required. The review also is assessing the level of training and support provided to the USAOs in developing the plans and efforts the USAOs made to test the plans to ensure their effectiveness.

#### Payments to Vendors

The OIG is reviewing the USAOs' controls and procedures over the purchase and payment for goods and services using third-party drafts, government purchase cards, electronic fund transfers, or Treasury checks to ensure that vendor payments are made according to the policies prescribed by the EOUSA and federal regulations.

## Bureau of Alcohol, Tobacco, Firearms and Explosives

The ATF is responsible for the enforcement of the federal laws relating to firearms, explosives, and arson and administers the U.S. Criminal Code provisions concerning alcohol and tobacco smuggling and diversion. It also seeks to combat terrorism, prevent crime, conduct fair and effective industry regulation and provides training and expertise to federal, state, local, and international law enforcement partners. *The Homeland Security Act of 2002* transferred these enforcement activities, along with certain other functions, to the Department of Justice from the Department of the Treasury. The ATF's approximately 4,800 special agents, inspectors, regulatory specialists, forensic auditors, laboratory technicians, and other personnel work primarily in 23 field divisions across the 50 states and in offices in Guam, the U.S. Virgin Islands, Puerto Rico, Mexico, Canada, Colombia, and France.

### Ongoing Work

#### The Federal Firearms Licensee Inspection Program

The OIG is examining the effectiveness of ATF's enforcement of federal firearms laws through its federal firearms licensee inspection program and the extent to which the program prevents the illegal transfer of firearms to those prohibited from having them. The review is assessing whether the program is effectively ensuring compliance with federal firearms laws and how program violations are identified and corrected.

# Top Management Challenges

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

The OIG's list of top challenges for 2003 is below. The list is not presented in order of priority. However, it is clear that the top challenge this year, as on last year's list, is the Department's ongoing response to the threat of terrorism.

Eight of the challenges from last year's list remain. They are long-standing, difficult issues that will not be solved quickly or easily.

We have added two new top challenges this year: (1) Protecting the Security of Department Information and Infrastructure and (2) Reducing the Supply of and Demand for Illegal Drugs. Maintaining the security of classified information and protecting critical infrastructure is a key challenge for the Department, as revealed by the Hanssen spy case and several ongoing OIG reviews. The other new challenge – reducing the supply of illegal drugs, the diversion of legal drugs for illicit use, and the demand for drugs in this country – is a critical challenge facing the Department and the nation.

## Top Management Challenges in the Department of Justice – 2003

1. Counterterrorism
2. Sharing of Intelligence and Law Enforcement Information
3. Information Systems Planning and Implementation
4. Computer Systems Security
5. Protecting the Security of Department Information and Infrastructure
6. Financial Management
7. Grant Management
8. Performance-Based Management
9. Human Capital
10. Reducing the Supply of and Demand for Illegal Drugs

Detailed information about these management challenges can be found at [www.usdoj.gov/oig/challenges.htm](http://www.usdoj.gov/oig/challenges.htm).

# Congressional Testimony

During this reporting period, the IG testified twice before congressional oversight committees and once before a congressionally chartered commission. He also submitted a written statement in connection with another congressional hearing.

- ◆ **Treatment of Aliens Held on Immigration Charges in Connection With the Investigation of the September 11 Attacks:** The IG testified on June 25, 2003, at a hearing called by the Senate Judiciary Committee to discuss the OIG's report that examined the Department's treatment of September 11 detainees. The IG summarized the major findings and 21 recommendations from the OIG's 198-page report released earlier that month (described in detail earlier in this semiannual report).
- ◆ **Follow-Up Review of Implementation of the Foreign Student Tracking Program:** During an April 2, 2003, hearing before the House Judiciary Committee, Subcommittee on Immigration, Border Security, and Claims, the IG discussed the OIG's follow-up review that examined the INS's progress in implementing its foreign student tracking system called SEVIS. The OIG review found that while the INS

had made significant progress implementing SEVIS, including requiring previously approved schools to reapply for certification and requiring non-accredited vocational, language, and flight schools to undergo on-site reviews, SEVIS was not yet fully implemented and significant deficiencies remain in its implementation.

- ◆ **Border Security Issues Post-September 11:** On April 1, 2003, the IG testified before the National Commission on Terrorist Attacks Upon the United States at its initial public hearing in New York City. The IG's testimony focused on OIG reviews involving border security, immigration, and other national security issues relevant to the Commission's work.
- ◆ **Reducing Waste, Fraud, and Abuse in Government Programs:** The IG submitted written testimony in connection with a July 9, 2003, oversight hearing before the House Committee on the Budget. The testimony described the results of OIG reviews that examined issues related to waste, fraud, and abuse, including Department procurement, grant management, and information technology systems planning and implementation activities.

# Legislation and Regulations

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

affects it and legislation that relates to waste, fraud, or abuse in the Department's programs or operations. During this reporting period, the OIG reviewed a variety of legislation, including a House bill to reauthorize the Department for FYs 2004 through 2006.

# Statistical Information

## Audit Statistics

### Audit Summary

During this reporting period, the Audit Division issued 238 audit reports containing more than \$25 million in questioned costs and \$1.4 million in funds to better use and made 313 recommendations for management improvement. Specifically, Audit issued 20 internal reports of programs funded at more than \$846 million; 15 external reports of contracts, grants, and other agreements

funded at more than \$59 million; 110 audits of bankruptcy trustees with responsibility for funds of more than \$197 million; and 93 *Single Audit Act* audits. In addition, the Audit Division issued six Notifications of Irregularities and nine Management Letter Transmittals.

### 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	12	\$15,643,824
Issued during period	5	\$1,497,136
Needing management decision during period	17	\$17,140,960
Management decisions made during period:		
◆ Amounts management agreed to put to better use <sup>1</sup>	13	\$10,161,693
◆ Amounts management disagreed to put to better use	2	\$3,473,052
No management decision at end of period	2	\$3,506,215

<sup>1</sup> 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	24	\$26,696,455	\$2,685,795
Issued during period	36	\$25,606,012	\$13,563,491
Needing management decision during period	60	\$52,302,467	\$16,249,286
Management decisions made during period:			
◆ Amount of disallowed costs <sup>1</sup>	38 <sup>2</sup>	\$29,490,601	\$9,352,644
◆ Amount of costs not disallowed	4	\$4,359,250	\$36,305
No management decision at end of period	20	\$18,452,616	\$6,860,337

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

<sup>2</sup> Two audit reports were not resolved during this reporting period because management has agreed with some, but not all, of the questioned costs in the audits.

## 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	30	91
Issued during period	103	313
Needing management decision during period	133	404
Management decisions made during period:		
◆ Number management agreed to implement <sup>1</sup>	107 <sup>2</sup>	343
◆ Number management disagreed with	0	0
No management decision at end of period	29	61

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

<sup>2</sup> Includes three audit reports that were not resolved during this reporting period because management has agreed to implement a number of, but not all, recommended management improvements in these audits.

## Audit Follow-Up

### OMB Circular A-50

OMB Circular A-50, *Audit Follow-Up*, requires audit reports to be resolved within six months of the audit report issuance date. The OIG monitors the status of open audit reports to track the audit resolution and closure process. As of September 30, 2003, the OIG had closed 221 audit reports and was monitoring the resolution process of 444 open audit reports.

## Unresolved Audits

### Audits Over Six Months Old Without Management Decisions

As of September 30, 2003, the following audits had no management decision or were in disagreement:

- ◆ COPS Grants to American University
- ◆ COPS Grants to the Albuquerque, New Mexico, Police Department
- ◆ COPS Grants to the Amtrak Police Department
- ◆ COPS Grants to the Baltimore County, Maryland, Police Department
- ◆ COPS Grants to the Camden, New Jersey, Police Department
- ◆ COPS Grants to the Chicago, Illinois, Police Department
- ◆ COPS Grants to the Dona Ana County, New Mexico, Sheriff's Department
- ◆ COPS Grants to the Frederick County, Maryland, Sheriff's Department
- ◆ COPS Grants to the Merced, California, Sheriff's Department
- ◆ COPS Grants to the Milpitas, California, Police Department

- ◆ COPS Grants to the Modesto, California, Police Department
- ◆ COPS Grants to the Picuris Pueblo, New Mexico, Police Department
- ◆ COPS Grants to the Prince William County, Virginia, Police Department
- ◆ COPS Grants to the Texas Tech University Police Department, Lubbock, Texas
- ◆ Independent Evaluation Pursuant to the Government Information Security Reform Act Fiscal Year 2001 – The Federal Bureau of Investigation Headquarters and Clarksburg, West Virginia, Data Centers Administrative and Investigative Mainframe Systems
- ◆ U.S. Marshals Service Intergovernmental Service Agreement for Detention Facilities with the Government of Guam

## Unresolved Inspections

DOJ Order 2900.10, *Follow-Up and Resolution Policy for Inspection Recommendations by the OIG*, requires reports to be resolved within six months of the report issuance date. As of September 30, 2003, there were no unresolved recommendations.

# Investigations Statistics

The following chart summarizes the workload and accomplishments of the Investigations Division during the 6-month period ending September 30, 2003.

## Source of Allegations

Hotline (telephone and mail)	653
Other sources	3,242
Total allegations received	3,895

## Investigative Caseload

Investigations opened this period	225
Investigations closed this period	272
Investigations in progress as of 9/30/03	479

## Prosecutive Actions

Criminal indictments/informations	71
Arrests	83
Convictions/Pleas	74

## Administrative Actions

Terminations	13
Resignations	56
Disciplinary action	17

## Monetary Results

Fines/Restitutions/Recoveries	\$1,287,599
Bribe monies deposited to the Treasury	\$7,344

## Integrity Awareness Briefings

OIG investigators conducted 38 Integrity Awareness Briefings for Department employees throughout the country during this reporting period for more than 1,675 employees. 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.



# Appendix 1

## AUDIT DIVISION REPORTS

**April 1, 2003 – September 30, 2003**

### INTERNAL AND EXTERNAL AUDIT REPORTS

Assets Forfeiture Fund and Seized Asset Deposit Fund Annual Financial Statement for Fiscal Year 2002

COPS Grants to the Asbury Park, New Jersey, Police Department

COPS Grants to the Cecil County, Maryland, Sheriff's Department

COPS Grants to the City of Chesapeake, Virginia, Police Department

COPS Grants to the City of Suffolk, Virginia, Police Department

COPS Grants to the Clark County Sheriff's Office, Vancouver, Washington

COPS Grants to the Cobb County, Georgia, Police Department

COPS Grants to the Connecticut Department of Public Safety, Division of State Police

COPS Grants to the District of Columbia Housing Authority Police Department

COPS Grants to the Henrico County, Virginia, Division of Police

COPS Grants to the Irvine, California, Police Department

COPS Grants to the National City, California, Police Department

COPS Grants to the Providence, Rhode Island, Police Department

COPS Grants to the University of Maine at Augusta

COPS Grants to the Yuba County, California, Sheriff's Department

Drug Enforcement Administration Annual Financial Statement for Fiscal Year 2002

Drug Enforcement Administration's Implementation of the Government Performance and Results Act

Federal Bureau of Investigation Annual Financial Statement for Fiscal Year 2002

Federal Bureau of Investigation Casework and Human Resource Allocation

Federal Bureau of Investigation's Implementation of Information Technology Recommendations

Federal Bureau of Prisons Annual Financial Statement for Fiscal Year 2002

Federal Bureau of Prisons Procurement Activities for Prison Space in California City, California

Federal Prison Industries, Inc. Annual Financial Statement for Fiscal Year 2002

Follow-up Audit of the Department of Justice Counterterrorism Fund

Immigration and Naturalization Service Annual Financial Statement for Fiscal Year 2002

Independent Evaluation Pursuant to the Government Information Security Reform Act for Fiscal Year 2002 – The Department of Justice Information Security Program and Practices Consolidated Report

Office of Justice Programs Annual Financial Statement for Fiscal Year 2002

Offices, Boards and Divisions Annual Financial Statement for Fiscal Year 2002

Select Application Controls of the Federal Bureau of Prisons's SENTRY Database System

Streamlining of Administrative Activities and Federal Financial Assistance Functions in the Office of Justice Programs and the Office of Community Oriented Policing Services

Superfund Activities in the Enforcement and Natural Resources Division for Fiscal Years 2000 and 2001

The September 11 Victim Compensation Fund of 2001

United States Marshals Service Annual Financial Statement for Fiscal Year 2002

Use of Equitable Sharing of Revenues by the Compton, California Police Department

Working Capital Fund Annual Financial Statement for Fiscal Year 2002

## TRUSTEE AUDIT REPORTS

Performed under a reimbursable agreement with the  
Executive Office for U.S. Trustees

Chapter 7 Trustee Theodore Albert	Chapter 7 Trustee Eugene R. Crane
Chapter 7 Trustee Lindy L. Allen	Chapter 7 Trustee Gregory K. Crews
Chapter 7 Trustee Monique Almy	Chapter 7 Trustee Allan J. DeMars
Chapter 7 Trustee Farley K. Banks	Chapter 7 Trustee John O. Desmond
Chapter 7 Trustee Michael G. Berland	Chapter 7 Trustee Daniel M. Donahue
Chapter 7 Trustee Amy L. Bostic	Chapter 7 Trustee Christian H. Dribusch
Chapter 7 Trustee Martha Bowman	Chapter 7 Trustee Michael C. Dunbar
Chapter 7 Trustee Scott W. Bradshaw	Chapter 7 Trustee Roberta S. Dunlap
Chapter 7 Trustee Lois I. Brady	Chapter 7 Trustee Marcia T. Dunn
Chapter 7 Trustee Roger W. Brown	Chapter 7 Trustee Barbara A. Edwards
Chapter 7 Trustee Steven Carr	Chapter 7 Trustee Karen E. Evangelista
Chapter 7 Trustee Carolyn R. Chaney	Chapter 7 Trustee Jerrold D. Farinash
Chapter 7 Trustee Julia A. Christians	Chapter 7 Trustee James S. Feltman
Chapter 7 Trustee Michael P. Cielinski	Chapter 7 Trustee Mark H. Flener
Chapter 7 Trustee Mark J. Conway	Chapter 7 Trustee Daniel E. Forsch

Chapter 7 Trustee Randall L. Frank	Chapter 7 Trustee Dennis W. King
Chapter 7 Trustee Maureen Gaughan	Chapter 7 Trustee Kenneth Kirschenbaum
Chapter 7 Trustee Robert Geltzer	Chapter 7 Trustee Yvette G. Kleven
Chapter 7 Trustee Virginia E. George	Chapter 7 Trustee Gina B. Krol
Chapter 7 Trustee Karen R. Goodman	Chapter 7 Trustee Elliott D. Levin
Chapter 7 Trustee Lauren P. Greene	Chapter 7 Trustee Jeffrey A. Levingston
Chapter 7 Trustee Jeanne B. Gregory	Chapter 7 Trustee David E. Lewis
Chapter 7 Trustee Paul D. Gresk	Chapter 7 Trustee Larry Liebzeit
Chapter 7 Trustee Maurice K. Guinn	Chapter 7 Trustee K. Jin Lim
Chapter 7 Trustee Joel C. Hall	Chapter 7 Trustee Jay Lubetkin
Chapter 7 Trustee Brenda Porter Helms	Chapter 7 Trustee John W. Luster
Chapter 7 Trustee Maxie E. Higgason	Chapter 7 Trustee Stanley G. Makoroff
Chapter 7 Trustee W. Ryan Hovis	Chapter 7 Trustee Joseph D. Marchand
Chapter 7 Trustee Michael J. Iannacone	Chapter 7 Trustee James R. Marshall
Chapter 7 Trustee Robert Johns	Chapter 7 Trustee Randy G. McKee
Chapter 7 Trustee James Joseph	Chapter 7 Trustee John Menchaca
Chapter 7 Trustee Steven Kartzman	Chapter 7 Trustee David L. Miller

Chapter 7 Trustee  
Jeffrey H. Mims

Chapter 7 Trustee  
Wilfredo Segarra Miranda

Chapter 7 Trustee  
Louis Movitz

Chapter 7 Trustee  
David E. Mullis

Chapter 7 Trustee  
Terry R. Nealey

Chapter 7 Trustee  
Joseph Newman

Chapter 7 Trustee  
Norman B. Newman

Chapter 7 Trustee  
Steven Notinger

Chapter 7 Trustee  
James R. Paris

Chapter 7 Trustee  
William J. Rameker

Chapter 7 Trustee  
Susan L. Rhiel

Chapter 7 Trustee  
David Rice

Chapter 7 Trustee  
Robert E. Ridgway

Chapter 7 Trustee  
Richard W. Roeder

Chapter 7 Trustee  
Roger Scholssberg

Chapter 7 Trustee  
Helen G. Schwartz

Chapter 7 Trustee  
Peter R. Scribner

Chapter 7 Trustee  
Anita L. Shodeen

Chapter 7 Trustee  
Christine Shubert

Chapter 7 Trustee  
Cynthia V.R. Skeen

Chapter 7 Trustee  
Timothy P. Smith

Chapter 7 Trustee  
W. Steve Smith

Chapter 7 Trustee  
Barry L. Solomon

Chapter 7 Trustee  
Steven L. Speth

Chapter 7 Trustee  
Thomas D. Stalnaker

Chapter 7 Trustee  
Janice A. Steinle

Chapter 7 Trustee  
Michael A. Stevenson

Chapter 7 Trustee  
James J. Stumpf

Chapter 7 Trustee  
William J. Tabor

Chapter 7 Trustee  
Harold S. Taxel

Chapter 7 Trustee  
Stephen B. Tayman

Chapter 7 Trustee  
Donald A. Thacker

Chapter 7 Trustee  
Allen Togut

Chapter 7 Trustee  
Donald W. Torgenrud

Chapter 7 Trustee  
Elizabeth A. Vaughan

Chapter 7 Trustee  
James R. Walsh

Chapter 7 Trustee  
Yvette Weinstein

Chapter 7 Trustee  
Kenneth A. Welt

Chapter 7 Trustee  
Henry Wheeler

Chapter 7 Trustee  
William D. White

Chapter 7 Trustee  
Russell L. Wilkey

Chapter 7 Trustee  
Richard A. Wilson

Chapter 7 Trustee  
David F. Wurst

Chapter 7 Trustee  
Mary T. Wynne

Chapter 7 Trustee  
Rudolph O. Young

Chapter 7 Trustee  
Nancy Zamora

## SINGLE AUDIT ACT REPORTS OF DEPARTMENT OF JUSTICE ACTIVITIES

Blackfeet Tribe of the Blackfeet Indian Reservation, Montana	Legislative Service Bureau
Boys and Girls Club of Syracuse, Inc.	Levy County, Florida
Butler County, Kansas	Makah Tribal Council, Washington
Camden Neighborhood Renaissance	Massachusetts Society for the Prevention of Cruelty to Children
Carteret County, North Carolina	Mississippi Coalition Against Sexual Assault, Inc.
Catholic Charities of the Archdiocese of Miami, Inc.	Montgomery County, Texas
Church World Service, Inc.	Municipality of Manati, Puerto Rico
Commonwealth of Kentucky	Municipality of Murrysville, Pennsylvania
Commonwealth of Puerto Rico Administration of Correction	Municipality of San Juan, Puerto Rico
Cook County, Illinois	National Association of Attorneys General, Washington, D.C.
Crisis Center for Women, Inc.	National Association of Drug Court Professionals, Alexandria, Virginia
D.A.R.E. America	National Association of State Fire Marshals
Dallas County, Texas	National Council on Alcoholism and Drug Dependence of Southwest Jersey, Inc.
District of Columbia Department of Corrections, Washington, D.C.	National Crime Prevention Council
District of Columbia Public Safety Cluster, Washington, D.C.	Neumann College
Gospel Rescue Ministries of Washington, D.C.	Old Lycoming Township, Pennsylvania
Havasuphi Tribe, Arizona	Osage Tribal Council
Indian Township Tribal Government	Ouachita, Louisiana Parish Sheriff
Joint Programs of the Shoshone and Arapaho Tribes of the Wind River Reservation, Wyoming	Potter County, Texas
Josephine County, Oregon	Salt Lake County, Utah
Kane County, Illinois	Sandoval County, New Mexico
Lawrence County, Indiana	Sangamon County, Illinois
	Sarasota County, Florida

South Dakota Coalition Against Domestic Violence and Sexual Assault

Suffolk County, New York

Sylvania Township, Lucas County, Ohio

Tangipahoa, Louisiana Parish Sheriff

Taos County, New Mexico

The City of Albany, New York

The City of Baltimore, Maryland

The City of Camden, New Jersey

The City of Chattanooga, Tennessee

The City of Decatur, Alabama

The City of Des Moines, Iowa

The City of Elizabeth, New Jersey

The City of Enterprise, Alabama

The City of Fairbanks, Alaska

The City of Fort Worth, Texas

The City of Gillette, Wyoming

The City of Greenville, South Carolina

The City of Greenville, Texas, FY 2001

The City of Greenville, Texas, FY 2002

The City of Irving, Texas, FY 1998

The City of Irving, Texas, FY 1999

The City of Johnstown, Pennsylvania

The City of Medford, Massachusetts

The City of Murfreesboro, Tennessee

The City of New York

The City of Pine Bluff, Arkansas

The City of Rutland, Vermont

The City of St. Paul, Minnesota

The City of Topeka, Kansas

The City of Waterbury, Connecticut, FY 2001

The City of Waterbury, Connecticut, FY 2002

The City of York, Pennsylvania

The Commonwealth of Massachusetts

The County of Norfolk, Massachusetts

The County of Plymouth, Massachusetts

The State of Alaska

The State of Florida, FY 2002

The State of Illinois

The State of New York, FY 2001

The State of New York, FY 2002

The State of North Carolina

The State of Texas

The Town of Seabrook, New Hampshire

The Town of Westford, Massachusetts

The Town of Yarmouth, Massachusetts

The Township of Old Bridge, New Jersey

Tunica County, Mississippi

White Buffalo Calf Woman Society, Inc., South Dakota



**AUDIT DIVISION REPORTS****April 1, 2003 – September 30, 2003**

<b>Quantifiable Potential Monetary Benefits</b>			
<b>Audit Report</b>	<b>Questioned Costs</b>	<b>Unsupported Costs</b>	<b>Funds Put to Better Use</b>
Blackfeet Tribe of the Blackfeet Indian Reservation, Montana	\$159,863	\$159,863	
Catholic Charities of the Archdiocese of Miami, Inc.	\$541,000		
Church World Service, Inc.	\$62,627	\$62,627	
Commonwealth of Puerto Rico Administration of Correction	\$35,126		
COPS Grants to Asbury Park, New Jersey, Police Department	\$1,294,490	\$1,226,395	\$238,181
COPS Grants to the City of Chesapeake, Virginia, Police Department	\$892,144		\$175,109
COPS Grants to the City of Suffolk, Virginia, Police Department	\$1,165,870		
COPS Grants to the Clark County Sheriff's Office, Vancouver, Washington	\$510,335		
COPS Grants to the Connecticut Department of Public Safety, Division of State Police			\$14,881
COPS Grants to the District of Columbia Housing Authority Police Department	\$9,586	\$9,586	
COPS Grants to the Henrico County, Virginia, Division of Police	\$562,033		
COPS Grants to the Irvine, California, Police Department			\$181,320
COPS Grants to the National City, California, Police Department	\$358,744		
COPS Grants to the Providence, Rhode Island, Police Department	\$2,790,491		\$887,645

<b>Audit Report</b>	<b>Questioned Costs</b>	<b>Unsupported Costs</b>	<b>Funds Put to Better Use</b>
COPS Grants to the University of Maine at Augusta	\$8,545	\$8,545	
COPS Grants to the Yuba County, California, Sheriff's Department	\$21,166		
Dallas County, Texas	\$735,960	\$735,960	
District of Columbia Public Safety Cluster, Washington, D.C.	\$242,637	\$217,137	
Follow-up Audit of the Department of Justice Counterterrorism Fund	\$3,071,271	\$1,439,341	
Gospel Rescue Ministries of Washington, D.C.	\$27,188		
Joint Programs of the Shoshone and Arapaho Tribes of the Wind River Reservation, Wyoming	\$7,376	\$7,376	
Mississippi Coalition Against Sexual Assault, Inc.	\$22,856		
Montgomery County, Texas	\$2,244,852	\$2,244,852	
National Association of State Fire Marshals	\$652	\$652	
National Council on Alcoholism and Drug Dependence of Southwest Jersey, Inc.	\$1,259	\$1,259	
Potter County, Texas	\$888		
Sarasota County, Florida	\$20,728		
The City of Elizabeth, New Jersey	\$500,000	\$500,000	
The City of Fort Worth, Texas	\$2,341,675	\$1,203,158	
The City of Irving, Texas, FY 1998	\$27,924		
The City of Waterbury, Connecticut, FY 2001	\$796,605	\$796,605	

<b>Audit Report</b>	<b>Questioned Costs</b>	<b>Unsupported Costs</b>	<b>Funds Put to Better Use</b>
The Commonwealth of Massachusetts	\$1,589,934	\$1,589,934	
The County of Plymouth, Massachusetts	\$463,685	\$463,685	
The State of Alaska	\$57,622	\$57,622	
The State of Illinois	\$2,201,986		
The State of New York, FY 2001	\$595,523	\$595,523	
The State of Texas	\$71,331	\$71,331	
Use of Equitable Sharing of Revenues by the Compton, California Police Department	\$2,172,040	\$2,172,040	
<b>Total</b>	<b>\$25,606,012</b>	<b>\$13,563,491</b>	<b>\$1,497,136</b>

## 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.

**Decision Unit:** A specific activity or project identified in an agency's annual budget.

**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 information technology, and financial statements. Internal audits are conducted in accordance with the Comptroller General's *Government Auditing Standards* and related professional auditing standards.

**Material Weakness:** A failure in a system of control or a lack of control determined by the agency head to be important enough to be reported to the President and Congress. A weakness of this type could significantly impair fulfillment of an agency's mission; deprive the public of needed services; violate statutory or regulatory requirements; significantly weaken safeguards against waste, loss, unauthorized use or misappropriation of funds, property, or other assets; or result in a conflict of interest.

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

**Questioned Cost:** A cost that is questioned by the OIG because of (a) an alleged violation of a provision of a law, regulation, contract, grant, cooperative agreement, or other agreement or document governing the expenditure of funds; (b) a finding that, at the time of the audit, such cost is not supported by adequate documentation; or (c) 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 (a) reductions in outlays; (b) deobligation of funds from programs or operations; (c) withdrawal of interest subsidy costs on loans or loan guarantees, insurance, or bonds; (d) costs not incurred by implementing recommended improvements related to the operations of the entity, a contractor, or grantee; (e) avoidance of unnecessary expenditures noted in pre-award reviews of contract or grant agreements; or (f) any other savings that are specifically identified.

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

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

**Unqualified Opinion:** The judgment of the certified public accountant who has no reservation as to the fairness of the entity's financial statements.

**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

### ACRONYMS AND ABBREVIATIONS

The following are acronyms and abbreviations used in the report.

<b>ATF</b>	Bureau of Alcohol, Tobacco, Firearms and Explosives	<b>OMB</b>	Office of Management and Budget
<b>BOP</b>	Federal Bureau of Prisons	<b>OPR</b>	Office of Professional Responsibility
<b>COPS</b>	Office of Community Oriented Policing Services	<b>USAO</b>	U.S. Attorney's Office
<b>DEA</b>	Drug Enforcement Administration	<b>USMS</b>	U.S. Marshals Service
<b>Department</b>	U.S. Department of Justice	<b>USP</b>	U.S. Penitentiary
<b>DHS</b>	Department of Homeland Security		
<b>EOUSA</b>	Executive Office for U.S. Attorneys		
<b>FBI</b>	Federal Bureau of Investigation		
<b>FCI</b>	Federal Correctional Institution		
<b>FY</b>	Fiscal year		
<b>GPRA</b>	<i>Government Performance and Results Act of 1993</i>		
<b>IG</b>	Inspector General		
<b>IG Act</b>	<i>Inspector General Act of 1978, as amended</i>		
<b>INS</b>	Immigration and Naturalization Service		
<b>IT</b>	Information technology		
<b>JMD</b>	Justice Management Division		
<b>MDC</b>	Metropolitan Detention Center		
<b>OIG</b>	Office of the Inspector General		
<b>OJP</b>	Office of Justice Programs		

## Appendix 4

### Reporting Requirements Index

The IG Act specifies reporting requirements for semiannual reports. The requirements are listed below and indexed to the applicable pages.

<b>IG Act References</b>	<b>Reporting Requirements</b>	<b>Page</b>
Section 4(a)(2)	Review of Legislation and Regulations	31
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	5-30
Section 5(a)(2)	Significant Recommendations for Corrective Actions	5-29
Section 5(a)(3)	Prior Significant Recommendations Unimplemented	34
Section 5(a)(4)	Matters Referred to Prosecutive Authorities	14-15, 19-20, 23-25, 27-28
Section 5(a)(5)	Refusal to Provide Information	None
Section 5(a)(6)	Listing of Audit Reports	36-46
Section 5(a)(7)	Summary of Significant Reports	5-29
Section 5(a)(8)	Audit Reports – Questioned Costs	33
Section 5(a)(9)	Audit Reports – Funds to Be Put to Better Use	32
Section 5(a)(10)	Prior Audit Reports Unresolved	34
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 4322  
Washington, DC 20530

**E-mail:** [oig.hotline@usdoj.gov](mailto:oig.hotline@usdoj.gov)

**Hotline:** (800) 869-4499

**Hotline fax:** (202) 616-9898

---

# Report Violations of Civil Rights and Civil Liberties

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

**Civil Rights & Civil Liberties Complaints  
Office of the Inspector General**

U.S. Department of Justice  
950 Pennsylvania Avenue, NW  
Room 4322  
Washington, DC 20530

**E-mail:** [inspector.general@usdoj.gov](mailto: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](http://www.usdoj.gov/oig).

Additional materials are available through the Inspectors General Network at [www.ignet.gov](http://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





This year marks the 25<sup>th</sup> anniversary of the *Inspector General Act*, which established the duties, responsibilities, and authorities of federal Inspectors General in 1978. Today, there are 57 Inspectors General in the federal government.

Department of Justice  
Office of the Inspector General

Established April 14, 1989