**U.S. Department of Justice**

FY 2011 PERFORMANCE BUDGET
Congressional Submission

# Office of the Inspector General

Table of Contents

## I. Overview for Office of the Inspector General

The Office of the Inspector General (OIG) was statutorily established in the Department of Justice (Department) on April 14, 1989. The OIG investigates allegations of fraud, waste, abuse, and misconduct by Department employees, contractors, and grantees and promotes economy and efficiency in Department operations. The OIG is an independent entity within the Department that reports to both the Attorney General and Congress on issues that affect the Department's personnel or operations.

The OIG has jurisdiction over all complaints of misconduct against Department employees in the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), Federal Bureau of Prisons (BOP), U.S. Marshals Service (USMS), Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), U.S. Attorneys' Offices (USAO), Office of Justice Programs (OJP), and other Offices, Boards and Divisions. The OIG investigates alleged violations of criminal and civil law, 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 efficacy.

In fiscal year (FY) 2010, the Department's budget proposal signaled a commitment to continue strengthening national security efforts while increasing support for the Department's traditional missions in the fight against crime. In FY 2010, the Department plans to devote approximately 90 percent of its resources to national security programs and traditional missions in law enforcement and litigation, while the remaining 10 percent funds state and local assistance programs. As part of its $27.7 billion budget for FY 2010, more than $8 billion is for protecting the American people from terrorist acts, and more than $2 billion will go towards information technology (IT) investments. The OIG, through its audits, inspections, investigations, and reviews, will help assure Congress and the taxpayers that the substantial funding provided to support these Department priorities and infrastructure investments are used efficiently, effectively, and for their intended purposes.

The OIG is committed to assisting the Attorney General and Congress in overseeing the use of counterterrorism resources, improving sharing of intelligence and law enforcement information, combating cybercrime, ensuring the security of computer systems, and improving management, accountability, and transparency of the Department's programs. **The OIG's request for FY 2011 totals $88.792 million, 503 positions, and 487 direct workyears.** This request represents an adjustment-to-base increase of $3.594 million; a program increase for 8 positions, 4 workyears, and $609,000 for enhanced oversight of the Department's national security programs; and a program increase of $394,000 for funding the operations of the Council of the Inspectors General for Integrity and Efficiency (CIGIE).

The OIG helps the Department pursue its strategic goals and objectives through its audits, investigations, inspections, and program reviews. The OIG has two general goals that support the Department's strategic goals: "detect and deter misconduct in programs and operations within or financed by the Department," and "promote the efficiency and effectiveness of Department programs and operations." To meet the first goal, the OIG targets investigative resources on allegations of fraud, bribery, civil rights violations, theft, sexual crimes, and official misconduct against Department employees or others who conduct business with the Department.

To meet the second goal, the OIG aims resources on reviews of Department programs to promote the economy, efficiency, and efficacy of those programs.

Like other organizations, the OIG must confront a variety of internal and external challenges that affect its work and impede progress towards achievement of its goals. These include the decisions Department employees make while carrying out their numerous and diverse duties, which affects the number of allegations the OIG receives, Department support for the OIG's mission, and financial support from the Office of Management and Budget (OMB) and Congress.

The OIG's biggest internal challenge in FY 2011 will be in the area of human capital. In this regard, the OIG must use all available recruitment tools and hiring flexibilities in a competitive job market to attract – and keep – top talent. Maintaining an optimal, committed workforce is critical to the OIG's overall performance and ability to achieve desired results. The OIG's focus on ensuring that its employees have the appropriate analytical and technological skills for the OIG's complex mission will bolster its reputation as a premier federal workplace and improve retention and results.

Electronic copies of the Department of Justice's Congressional Budget Justifications and Capital Asset Plan and Business Case exhibits can be viewed or downloaded from the Internet using the Internet address: **http://www.usdoj.gov/jmd/2011justification/**.

## II. Summary of Program Changes

| Office of the Inspector General ($ in thousands) | | | | | |
|---|---|---|---|---|---|
| **Item Name** | **Description** | **Pos.** | **FTE** | **Dollars** | **Page** |
| **Enhanced Oversight of DOJ's National Security Programs** | The OIG is requesting 4 program analysts and 4 auditors for enhanced oversight of the Department's national security programs, including assessing DOJ's Efforts to Address Terrorists' Financing; the Foreign Surveillance Intelligence Act (FISA) U.S. Persons Collections Program; the FBI's use of National Security Letters, 215 Orders, and FISA Pen Register Orders; the FBI's Efforts to Combat National Security Cyber Threats; and the operations of the FBI's Office of Integrity and Compliance. | **8** | **4** | **$609** | **42** |
| **CIGIE Operations** | The OIG is requesting funding for its annual share of supporting the governmentwide efforts and operations of the Council of the Inspectors General on Integrity and Efficiency (CIGIE). | | | **$394** | **44** |
| **Travel Savings and Efficiencies** | DOJ is focusing on travel as an area in which savings can be achieved. For the OIG, travel or other management efficiencies will result in offsets of $173,000. This offset will be applied in a manner that will allow the continuation of effective law enforcement program efforts in support of Presidential and Departmental goals, while minimizing the risk to health, welfare, and safety of agency personnel. | | | **($173)** | **45** |
| | **Total** | **8** | **4** | **$830** | |

## III. Appropriations Language and Analysis of Appropriations Language

### Appropriations Language

## OFFICE OF THE INSPECTOR GENERAL
## Salaries and Expenses

For necessary expenses of the Office of the Inspector General, [$84,368,000] *$88,792,000*, including not to exceed $10,000 to meet unforeseen emergencies of a confidential character.

### Analysis of Appropriations Language

No substantive changes proposed.

## IV. Decision Unit Justification

### A. Audits, Inspections, Investigations, and Reviews

The OIG operates as a single decision unit encompassing audits, inspections, investigations, and reviews.

| OIG | Perm. Pos. | FTE | Amount |
|---|---|---|---|
| 2009 Enacted | 450 | 438 | $75,681,000 |
| 2009 Supplemental | | | $2,000,000 |
| 2009 Enacted with Supplementals | 450 | 438 | $77,681,000 |
| 2010 Request | 495 | 474 | $84,368,000 |
| Adjustments to Base and Technical Adjustments | | 9 | $3,594,000 |
| 2011 Current Services | 495 | 483 | $87,962,000 |
| 2011 Program Increases | 8 | 4 | $1,003,000 |
| 2011 Program Decreases | | | ($173,000) |
| 2011 Request | 503 | 487 | $88,792,000 |
| **Total Change 2010-2011** | **8** | **13** | **$4,424,000** |

**Note:** The FTEs above do not include reimbursables.

### 1. Program Description

The OIG operates as a single decision unit encompassing audits, inspections, investigations, and reviews.

| OIG-Information Technology (IT) Breakout (of Decision Unit Total) | Perm. Pos. | FTE | Amount |
|---|---|---|---|
| 2009 Enacted | 11 | 11 | $4,921,000 |
| 2009 Supplemental | | | |
| 2009 Enacted with Supplementals | 11 | 11 | $4,921,000 |
| 2010 Request | 11 | 11 | $5,057,000 |
| Adjustments to Base and Technical Adjustments | | | |
| 2010 Current Services | 11 | 11 | $5,193,000 |
| 2011 Program Increases | | | |
| 2011 Request | 11 | 11 | $5,193,000 |
| **Total Change 2010-2011** | **0** | **0** | **$136,000** |

The OIG has no IT investment request for FY 2011.

## 2. Performance Measures

Because of the nature of its work, the OIG provides both qualitative (narrative) and quantitative performance information to better enable the Department, Congress, and the public to assess the value of the work it performs.

The OIG does not set targets for certain law enforcement activities since those measures could be construed as "bounty hunting." Instead, the OIG reports historical results for these measures.

In addition, consistent with previous budget submissions, the performance indicators cover all of the OIG's programs, whether funded from direct appropriations or reimbursements.

**Examples of Recent OIG Reviews**

**FBI's Use of Exigent Letters**

In January 2010, the OIG released a report examining the extent of the FBI's use of exigent letters to obtain telephone records without legal process. The report also identified, for the first time, other informal requests that the FBI used to obtain telephone records improperly. In addition, the report examines the accountability of FBI employees, supervisors, and managers who were responsible for these flawed practices.

Two previous reports by the OIG, issued in March 2007 and March 2008, generally described the FBI's misuse of national security letters to obtain sensitive records. In those reports, we noted the FBI's practice of issuing exigent letters, instead of national security letters (NSLs) or other legal process, to obtain telephone records from three communications service providers. The exigent letters requested telephone records based on alleged "exigent circumstances," and often inaccurately stated that grand jury subpoenas already had been sought for the records. Our previous reports concluded that the FBI's practice of using exigent letters circumvented the requirements of the Electronic Communications Privacy Act (ECPA) statute governing national security letters, and violated Attorney General Guidelines and FBI policy.

The January 2010 report examines in more detail the use of exigent letters for telephone records that did not comply with legal requirements or FBI policies governing the acquisition of these records. The report also provides significant new details about how the FBI's practice of using exigent letters evolved, how widespread it became, and the management failures that allowed it to occur. The OIG report also identifies other informal ways, in addition to the exigent letters, by which the telephone service providers gave telephone records to the FBI without legal process. For example, the FBI asked for and obtained telephone records through requests by e-mail, face-to-face, on post-it notes, and by telephone. The FBI also obtained telephone records using a practice referred to by the FBI and the providers as "sneak peeks."

Additionally, the report describes, also for the first time, three FBI media leak investigations in which the FBI sought, and in two cases received, records or calling activity information for telephone numbers assigned to reporters, without first obtaining required approval from the Attorney General.

The OIG report describes how the FBI issued over 700 exigent letters seeking records on more than 2,000 different telephone numbers from 2003 to 2006. Nearly all of these letters referenced "exigent circumstances" as the basis for the request and asserted that a grand jury subpoena or other legal process had been sought for the records.

In some cases, these exigent letters were used in urgent investigations. But the OIG's investigation found that, contrary to the statements in the letters, many of the investigations for which the letters were used did not involve emergency or life-threatening circumstances (the standard required under the ECPA for voluntary disclosure), and, also contrary to the letters, subpoenas had not been sought for the records. Moreover, there was no process by which a supervisor reviewed and approved the issuance of exigent letters. In fact, FBI personnel were not even required to retain a copy of the exigent letter.

The use of exigent letters was just one of the many improper practices described in the OIG's report. The OIG's investigation also found widespread use of even more informal requests for telephone records in lieu of appropriate legal process or a qualifying emergency. The scope and variety of these informal requests was startling.

For example, the OIG found that, rather than using NSLs, other legal process, or even exigent letters, FBI personnel sought and received telephone records based on informal requests made by e-mail, by telephone, face-to-face, and even on post-it notes. The OIG found that the FBI's Communications Analysis Unit (CAU) personnel made such informal requests for records associated with at least 3,500 telephone numbers, although we could not determine the full scope of this practice because of the FBI's inadequate record-keeping.

The OIG found that the FBI also improperly obtained telephone records through "sneak peeks," whereby the on-site communications service providers' employees would check their records and provide a preview of the available information for a targeted phone number, without documentation of any justification for the request from the FBI and often without documentation of the fact of the request. At times, the service providers' employees simply invited FBI personnel to view the telephone records on their computer screens.

Notably, virtually none of these FBI requests for telephone records – either the exigent letters or the other informal requests – was accompanied by documentation explaining the authority for the requests or the investigative reasons why the records were needed, and many of the requests lacked information as basic as date ranges. This resulted in the FBI obtaining substantially more telephone records covering longer periods of time than it would have obtained had it complied with the NSL process, including records that were not relevant to the underlying investigations. Many of these records were uploaded into FBI databases.

The OIG concluded that these and other informal processes described in the report represented an egregious breakdown in the FBI's responsibility to comply with the ECPA, the Attorney General Guidelines, and FBI policy.

The report also describes other troubling practices, such as the FBI's use of "community of interest" requests without first determining that the requested records were relevant to authorized investigations, and "hot number" requests that we believe also violated the ECPA. The OIG also uncovered misuse of FBI administrative subpoenas for telephone records. In addition, we found

that the FBI made inaccurate statements to the FISA Court. In several instances, the FBI submitted affidavits to the Court that information in FISA applications was obtained through NSLs or a grand jury subpoena, when in fact the information was obtained by other means, such as exigent letters.

The OIG investigation found that the close relationship between the FBI's CAU and the three communications service providers facilitated the casual culture surrounding the use of exigent letters and other informal requests for telephone records at the FBI. Employees of one or more of these service providers were physically located on-site in the FBI's CAU from April 2003 to January 2008. These employees, who were capable of querying company databases on request, were regarded by FBI personnel as members of the communications analysis "team."

In fact, the OIG found that the FBI's use of exigent letters became so casual, routine, and unsupervised that employees of all three communications service providers sometimes generated exigent letters for FBI personnel to sign and return to them. Although co-locating the service providers' employees at the FBI was originally an attempt to facilitate efficient and effective cooperation between the FBI and the service providers, the proximity fostered close relationships that blurred the line between the FBI and the service providers. The OIG concluded that this co-location, in combination with poor supervision and ineffective oversight, contributed to the serious abuses described in the report.

The OIG's investigation found that the FBI's initial actions to address the issues arising from the FBI's use of exigent letters and other informal requests were deficient and ill-conceived, including the FBI's attempts to issue 11 after-the-fact, "blanket" national security letters to "cover" or validate the improperly obtained telephone records. Only after the OIG issued its first NSL report in March 2007 did the FBI take appropriate steps to address the difficult problems that the deficient exigent letters practice had created.

Among the troubling incidents detailed for the first time in this report are three FBI media leak investigations in which the FBI sought, and in two cases received, telephone toll billing records or other calling activity information for telephone numbers assigned to reporters without first obtaining the approvals from the Attorney General that are required by federal regulation and Department policy. In one of these cases, the FBI loaded the records it obtained in response to an exigent letter into a database, where the records stayed for over 3 years. The records were not removed until OIG investigators determined that the records had been improperly obtained and we notified the FBI. The OIG report concluded that serious lapses in training, supervision, and oversight led to the FBI and the Department issuing these requests for the reporters' records without following legal requirements and their own policies.

The OIG report also assessed the accountability of individuals for these improper practices. We concluded that numerous, repeated, and significant failures led to the FBI's use of exigent letters and other improper requests for telephone records over an extended period of time. These failures began shortly after the CAU was established within the Counterterrorism Division in 2002, and they continued until March 2007 when the OIG issued its first NSL report describing the improper use of exigent letters. We concluded that every level of the FBI was responsible for these failures, from the FBI'S most senior officials, to attorneys in the Office of General Counsel, to counterterrorism managers, to the supervisors at the CAU, and to the CAU agents and analysts who repeatedly signed the letters and made the other informal requests.

In general, the OIG found that FBI officials' oversight of the use of exigent letters and other informal requests, and the FBI's initial attempts at corrective action, were seriously deficient, ill-conceived, and poorly executed. From 2003 through 2006, FBI officials repeatedly failed to take steps to ensure that the FBI's requests for telephone records were consistent with the ECPA, the Attorney General Guidelines, and Department policy. For three and a half years, FBI officials and employees issued hundreds of exigent letters, failing to object even to letters that contained inaccurate statements on their face. FBI supervisors also failed to develop and implement an effective system for tracking FBI requests for records or other information from the on-site providers.

FBI officials attempted to remedy the FBI's failure to serve legal process through legally deficient, after-the-fact blanket NSLs intended to "cover" the records it had previously requested. And when FBI attorneys became aware of the practice of using exigent letters, they failed to stop it, participated in the ill-conceived efforts to remedy the problem after the fact, and provided legal advice to the CAU that was inconsistent with the ECPA, the Attorney General Guidelines, and FBI policy.

The OIG's report discusses the accountability of individual FBI personnel for these failures. We assess the accountability of FBI employees who either signed the exigent letters or had a management or oversight role in the process, and we describe their role in the failures identified in this report. In the report, we recommend that the FBI review the conduct and performance of these individuals and determine whether discipline or other action with regard to each of them is appropriate.

After the OIG issued our first report in March 2007 on the FBI's misuse of national security letters, the FBI ended the use of exigent letters, issued clear guidance on the use of national security letters and on the proper procedures for requesting records in circumstances qualifying as emergencies under the ECPA, provided training on this guidance, moved the three service providers out of FBI offices, and expended significant effort to determine whether improperly obtained records should be retained or purged from FBI databases. The FBI should be credited for these actions.

However, as a result of further deficiencies uncovered in the OIG's review, we believe the FBI and the Department need to take additional action to ensure that FBI personnel comply with the statutes, guidelines, and policies governing the FBI's authority to request and obtain telephone records. Our report contains thirteen recommendations for additional action that the OIG believes is necessary to address the improper requests for telephone records uncovered during the OIG's investigation, and to ensure that the past abuses do not recur. For example, we recommend that the FBI issue periodic guidance and training relating to the authority of FBI employees to obtain telephone records, ensure that requests for information made pursuant to contracts with telephone service providers comply with federal law and Department policies, and implement other corrective action to address the findings of this report.

The January 2010 unclassified report released publicly contains information that is redacted because the FBI and the Intelligence Community consider that information to be classified. The redactions are noted in the report. Full classified reports, without redactions, were provided to the Department, the FBI, the Intelligence Community, and Congress.

**Oversight of Judicial Security**

In January 2010, the OIG issued a report examining the Department of Justice's (DOJ's) protection of federal judges and prosecutors. The OIG previously issued two reports on the United States Marshals Service's (USMS) protection of federal judges. In this report, we found that DOJ's threat response program continues to have deficiencies in several critical areas that affect the ability to protect federal judges, U.S. Attorneys, and Assistant U.S. Attorneys (AUSAs). Our report also found that threats and inappropriate communications to federal judges, U.S. Attorneys, and AUSAs have increased dramatically during the past several years, growing from 592 in fiscal year (FY) 2003 to 1,278 in FY 2008. Overall, during this 6-year period, there were 5,744 threats directed at these federal officials.

The USMS's district offices have primary responsibility for ensuring the safety and security of federal judicial proceedings and protecting more than 2,000 federal judges and approximately 5,250 other federal court officials, including U.S. Attorneys and AUSAs.

Two other Department components – the Executive Office for United States Attorneys (EOUSA) and the U.S. Attorneys' Offices (USAO) – are also involved in responding to these threats. EOUSA is responsible for providing oversight, guidance, and financial support to help the USAOs respond to threats against their employees. The USAOs are responsible for reporting threats against their employees to the USMS and EOUSA, and also provide some protective measures in response to threats.

Although no federal judge or AUSA was killed or seriously injured during the time period we reviewed, we nevertheless found numerous deficiencies in the USMS's and EOUSA's response to threats that affect their ability to protect federal officials.

We found that judges, U.S. Attorneys, and AUSAs do not consistently and promptly report threats, which hamper the ability of the USMS to protect these federal court officials from harm. Although we could not determine the precise number of unreported threats, our interviews and surveys indicate that as many as 25 percent of all threats or inappropriate communications were not reported to the USMS. We also found that in about one-quarter of the reported threats made in FY 2007 and FY 2008, 2 or more days elapsed between receipt of the threat by the judge or AUSA and when they reported the threat to the USMS. Our review recommended that the Department provide additional guidance to ensure that threats are reported promptly.

We found that when threats are reported, the USMS does not consistently perform or document risk assessments, and the USMS therefore cannot ensure that the protective measures provided to protectees are commensurate with the threats or that even the minimum protective measures are implemented. In reviewing a selected sample of 26 threat cases involving 25 judges and AUSAs, we found that the USMS did not record the risk level ratings for any of these threats in its threat database. Through our interviews and database review, we determined that only 1 of the 25 judges and AUSAs received all four protective measures called for by USMS protocols. In addition, five judges and AUSAs were not provided any of the low risk level protective measures they should have received.

We also found that the USMS does not fully or effectively coordinate with other law enforcement agencies to respond to threats against federal judicial officials. Our review determined that that 639 (40 percent) of the 1,587 threats in the USMS database contained no

information regarding FBI notification, even though such notification is required by USMS policy. USMS policy also requires USMS district offices to contact local law enforcement agencies to request that the USMS be notified whenever a police agency responds to any emergency call at a judge's residence. However, when we tested the USMS contact numbers provided in three of these letters, two of the letters had non-working USMS contact numbers.

In addition, we found that EOUSA and the USAOs have not implemented adequate measures to protect USAO personnel against threats. For example, we determined that many USAO staff members assigned security duties lack threat response expertise and training similar to that of the USMS's judicial security staff members, who are specifically trained in threat response procedures.

We also found that USAO and USMS staff responsible for responses to threats against U.S. Attorneys and AUSAs did not consistently share important information with each other and were not cognizant of each other's roles and responsibilities. Moreover, the USAOs are not consistently notifying EOUSA of threats against, or protective measures provided to, U.S. Attorneys and AUSAs, which prevents EOUSA from providing emergency support or tracking trends in threats against USAO personnel.

In this report, the OIG made 14 recommendations to improve the protection of federal judges and prosecutors, including recommendations to improve the guidance given to federal judges, U.S. Attorneys, and AUSAs on the need for prompt reporting of threats; to ensure that the USMS provides federal judicial officials with protective measures that are commensurate with the risk level of the threat; and to ensure better coordination between the USMS, the USAOs, and other law enforcement agencies who share responsibility for protecting federal judicial officials. The USMS and EOUSA stated that they concurred with all of our recommendations and have begun implementing corrective action.

**The FBI's Sentinel Case Management System**

In November 2009, the OIG released its fifth in a series of reports examining the FBI's ongoing development of its Sentinel case management project, which is intended to provide the FBI a fully electronic case management system and an automated workflow process.

This audit found that the FBI's development of Sentinel continues to progress, and the FBI has addressed most of the concerns identified in our previous four audit reports on Sentinel. However, in this audit we identified several new areas of concern with the overall progress of Sentinel and, in particular, the implementation of Phase 2 of the project.

As described in our audit report, the FBI previously awarded a contract to Lockheed Martin in March 2006 to develop Sentinel in four phases. As we reported in our last audit, the FBI has completed Phase 1, which provided FBI employees with web-based access to information currently in the FBI's Automated Case Support (ACS) System, as well as improved search capabilities.

In our four previous audit reports on Sentinel, we also highlighted various concerns about the development of Sentinel, such as the FBI's ability to track and control Sentinel's costs, the ability to reprogram funds without jeopardizing the FBI's other mission-critical operations, efforts to ensure that Sentinel will allow the sharing of information between the FBI and other

intelligence and law enforcement agencies, and lack of contingency planning for identified project risks that warranted continued monitoring by the FBI. Our current audit found that the FBI made progress in addressing most of the concerns identified in the OIG's previous four reports.

In this audit, however, we focused on the FBI's progress towards implementing Phase 2 of the project, which originally was intended to deliver eight electronic forms, implement more efficient work processes, and begin the migration of administrative case data currently in ACS to Sentinel. The FBI accepted delivery of Sentinel's Phase 2, Segment 3 in April 2009, which according to the FBI delivered: (1) interfaces to six FBI IT systems; (2) enhanced system administration; (3) portions of Sentinel's records management capability; (4) a user-friendly method of sending and receiving tasks; and (5) the ability to extract administrative case data from ACS.

This audit found that the delivered portions of Sentinel's Phase 2 did not provide significant additional functionality to FBI users as initially planned. In this phase, the FBI and Lockheed Martin encountered considerable challenges deploying new electronic versions of forms used by FBI agents during investigations that would meet security standards and user requirements. As a result, the FBI has adopted a new approach to developing forms and has deferred deployment of the forms from Phase 2 to later stages of the Sentinel project.

Moreover, we determined that while the FBI's estimate of Sentinel's overall cost has not increased from $451 million since we issued our last report in December 2008, the FBI now projects that Phase 2 will cost $155 million, or $18 million more than budgeted to complete. The FBI plans to reallocate costs from other project areas, including the management risk reserve, to offset the $18 million increase in Phase 2 development costs. In addition, as a result of the replanning of the remainder of Phase 2, some deliverables originally scheduled for Phase 2 have been deferred to later phases of the project.

Overall, the FBI's revised schedule extends the estimated completion date for Phase 2 of Sentinel to October 2009, 3 months later than previously reported. Consequently, the overall project completion date has been extended to September 2010, 3 months later than the FBI estimated at the time of our last audit report and 9 months later than originally planned. In addition to delays in developing new parts of Sentinel, FBI employees have expressed concerns about the current operation of Sentinel. Specifically, users frequently complained about the system's slow response time to requests for information. We found that the slow response times are primarily caused by the FBI's aging communications network architecture, which was last upgraded in 2002. In March 2009 the FBI began an upgrade of its computer network that is estimated to cost $39 million and is planned to be completed by December 2009. According to the FBI, the network upgrade should improve Sentinel's response time.

Finally, due to the aggressive schedule, scope, and importance of Sentinel's implementation, the project requires a highly skilled and integrated project management staff. We have concerns with the staffing of the project because of a recent increase in turnover among project staff members and vacancies within the Sentinel Project Management Office, and because the Sentinel staffing plan does not reflect the current staffing levels or skills needed for the project.

The OIG report made six recommendations to help the FBI manage development of the Sentinel case management system. These recommendations include increasing user involvement in the development of Sentinel, developing a goal for Sentinel's response time to user inputs, and filling vacancies at the Sentinel PMO. The FBI agreed with all six recommendations.

The OIG will continue to monitor Sentinel's progress and issue audit reports throughout the life of the project.

**Explosives Investigation Coordination Between the FBI and the ATF**

In October 2009, the OIG issued an audit report that found inadequate coordination on explosives investigations by the FBI and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and a lack of effective management by DOJ of these agencies' coordination efforts. Our report found that conflicts continue to occur throughout the country regarding which agency is the lead agency for federal explosives investigations and about their differing explosives-handling techniques.

Federal law gives the FBI and ATF concurrent jurisdiction over most federal explosives crimes. Despite attempts at coordination, these components have developed separate and often conflicting approaches to explosives investigations and related activities such as explosives training, information sharing, and forensic analysis. After ATF was transferred from the Department of the Treasury to DOJ in 2003, the Attorney General issued a Memorandum (the 2004 Memorandum) that attempted to define the roles of the FBI and ATF in explosives investigations and related activities.

However, our audit found that DOJ, the FBI, and ATF did not implement the 2004 Memorandum's procedures for explosives information sharing and database consolidation, training, and laboratory resources. We also found that the Memorandum contained ambiguous directives for determining lead agency authority for explosives matters. In addition, a subsequent 2008 Memorandum of Understanding between the FBI and ATF did not clarify investigative jurisdiction and instead reiterated many of the ambiguous elements of the 2004 Attorney General Memorandum.

Based on an OIG survey of ATF and FBI explosives specialists, field managers, and state and local bomb squads, as well as over 100 interviews of ATF and FBI employees in the field, our audit found that conflicts continue to occur between the FBI and ATF throughout the country regarding which agency should lead federal explosives investigations or which techniques should be used to neutralize explosives. Our survey found that 33 percent of ATF explosives specialists and 40 percent of FBI bomb technicians responding to our survey reported having disputes with their counterparts at explosives incidents between fiscal years 2007 and 2008.

Our audit found, for example, that the FBI and ATF sometimes race to be the first federal agency on the scene of an explosives incident. Disputes have occurred when one agency arrives first and the other agency believes the incident falls within its lead agency authority. These disputes can delay investigations, confuse local first responders about which agency is the federal lead on explosives matters, and also undermine federal and local relationships. In fact, we found that over three-quarters of explosives specialists at both ATF and the FBI who responded to our survey believed the other agency duplicated capabilities already on scene, delayed decision-making, and failed to provide important explosives or post-blast expertise.

The FBI and ATF still maintain separate explosives-related databases to manage laboratory forensic reports, incident reporting, and technical explosives-related information and intelligence. In particular, although the 2004 Memorandum required the FBI and ATF to consolidate their records of criminal explosives incidents reported by federal, state and local agencies into ATF's Bombing and Arson Tracking System (BATS), we found that the FBI only provided a one-time transfer of its explosives-incident data, and has not reported any subsequent explosives-incident information to BATS since 2004. The agencies' separate explosives databases cause a duplication of effort and the lack of reporting to the BATS database undermines the database's ability to accurately determine trends in explosives incidents. The 2004 Memorandum also directed ATF to coordinate all DOJ post-blast explosives training and certify all explosive detection canines deployed by DOJ components. However, the FBI and ATF have not implemented either directive. Instead, the FBI and ATF continue to separately operate their respective explosives-training facilities and programs, and they disagree on certain aspects of explosives training. In addition, the FBI and ATF each continue to maintain separate laboratories that perform explosives-related analyses, and the Department has not developed the guidance directed by the 2004 Memorandum on how resources and workloads should be allocated between the two agencies' laboratories.

The issues we found regarding lack of coordination between the FBI and ATF in explosives-related operations, database information consolidation and sharing, and explosive training also increase the risk that DOJ will not meet the requirements of Homeland Security Presidential Directive (HSPD)-19, which requires a unified, multi-layered strategy to mitigate the threat of and prevent the use of explosives by terrorists.

The OIG audit made 15 recommendations to DOJ, the FBI, and ATF to improve explosives-related coordination, including implementing a new DOJ directive that clearly defines jurisdiction between the agencies; establishing a formal procedure for DOJ to resolve jurisdictional disputes; requiring reviews of the most efficient uses of DOJ explosives training programs and laboratory resources; and issuing new agency guidelines to promote explosives-incident reporting and information sharing by both agencies. The Department said it agreed in concept with each of our recommendations, but did not provide specific information about how it intended to address each recommendation.

**DOJ's Anti-Gang Intelligence and Coordination Centers**

In November 2009, the OIG issued a report examining the two gang intelligence and coordination centers the Department established in 2006 to combat gang-operated criminal networks in the United States – the National Gang Intelligence Center (NGIC) and the National Gang Targeting, Enforcement, and Coordination Center (GangTECC). Our report concluded that the two centers have not significantly improved the coordination and execution of the Department's anti-gang initiatives.

According to the 2009 National Gang Threat Assessment, more than 1 million gang members – an increase of 200,000 since 2005 – belong to over 20,000 gangs that are criminally active within the United States. These gang networks are estimated to commit as much as 80 percent of the crime in some communities.

In January 2006, the National Gang Intelligence Center (NGIC) was established as a multi-agency center administered by the Federal Bureau of Investigation (FBI), where intelligence analysts from federal, state, and local law enforcement would work together to develop and share gang-related information. In June 2006, the Department of Justice (Department) formed the National Gang Targeting, Enforcement, and Coordination Center (GangTECC) to coordinate multi-jurisdictional gang investigations. GangTECC is administered by the Department's Criminal Division.

This OIG review examined the operations of these two centers. With regard to NGIC, we found that it has not established a centralized gang information database for collecting and disseminating gang intelligence, as directed by statute, because of technological limitations and operational problems. In addition, the communications infrastructure that would allow NGIC to access gang-related information from state databases had not progressed beyond the development phase.

We also found that NGIC has few regular users outside of the FBI and GangTECC, receives few requests for information, and produces reports that are of limited usefulness. For example, state, local, and tribal law enforcement agencies averaged only 3 requests per year and submitted only 13 of the 213 total requests for information received by NGIC from its inception in 2006 to February 2009.

In our discussions with NGIC and GangTECC personnel and other law enforcement officials about why NGIC was not used more frequently by law enforcement agencies, we found that NGIC was not perceived as an independent, multi-agency center by many law enforcement personnel, and it was repeatedly referred to as being "FBI-centric" in the products it generates and the intelligence analysis it provides. In addition, our interviews found that NGIC's intelligence products are considered to be of limited usefulness.

With regard to GangTECC, the OIG found that GangTECC has a broad, multi-purpose mission but no operating budget. The lack of an operating budget has prevented GangTECC managers from taking actions essential to its operations, including hosting case coordination meetings and conducting effective outreach to the law enforcement community. In addition, GangTECC has not established itself as the central coordination and deconfliction entity as envisioned because GangTECC's member agencies and federal prosecutors are not required to inform GangTECC of their gang-related investigations and prosecutions.

Finally, in examining the relationship between NGIC and GangTECC, we found that the two entities have not worked together effectively because of differing leadership and management philosophies, funding sources, and investigative priorities. While the two centers share an office suite, their co-location has not led to the anticipated partnership of NGIC and GangTECC, and communication between the two centers remains limited and ad hoc.

The OIG made 15 recommendations to improve the Department's anti-gang efforts, including to consider merging NGIC and GangTECC under common leadership to improve their ability to support and coordinate the Department's anti-gang initiatives on a national level. The Department responded by stating that it concurred in concept with all of the recommendations and it is taking steps to address the recommendations, including considering organizational changes. However, the OIG believes the Department needs to address each of the specific

recommendations, including whether to merge the two centers, and we have asked for a more specific response to the recommendations.

**The FBI's Foreign Language Translation Program**

In October 2009, the OIG issued an audit report that examined the FBI's Foreign Language Translation Program, focusing on the FBI's progress in improving its ability to translate and review material it collects.

In 2004 and 2005, the OIG issued audit reports on the FBI's translation program. These reviews found that significant amounts of audio material collected for FBI counterterrorism and counterintelligence operations were awaiting translation, including material collected for the FBI's highest priority cases.

For this audit, the OIG expanded its audit to include material collected for FBI criminal investigations, and we evaluated in more depth the FBI's review of its counterterrorism and counterintelligence audio, text, and electronic file material.

Our audit found that the FBI continued to have significant amounts of unreviewed material it collected for its counterterrorism, counterintelligence, and criminal investigations between fiscal years (FY) 2006 and 2008. While the FBI had reviewed 100 percent of the text pages it collected during this period, we found the FBI did not review 14.2 million (31 percent) of the 46 million electronic files that it collected during this same period. In addition, we found that the FBI did not review 1.2 million hours (25 percent) of the 4.8 million audio hours it collected for counterterrorism and counterintelligence operations between FYs 2003 and 2008.

For its counterterrorism audio collections, we found the FBI reviewed about 94 percent of the material it collected between FYs 2003 and 2008, which is similar to the 93 percent we reported in our previous audits. However, in terms of total hours the amount of unreviewed counterterrorism audio material increased from about 8,600 hours in FY 2003 to nearly 47,000 hours through FY 2008 because the amount of material collected by the FBI increased while at the same time the FBI failed to meet hiring goals for translators.

As in our previous audits of the FBI's foreign language translation program, we determined that significant portions of the FBI's unreviewed audio and electronic file material were collected for cases in its two highest-priority counterterrorism and counterintelligence categories. For example, in FY 2008 the FBI did not review 740 counterterrorism audio hours collected in English that pertained to its highest-priority category of cases. Additionally, the FBI did not review 2,800 counterterrorism audio hours and 150,000 counterintelligence hours for cases in its second highest-priority counterterrorism category. We concluded that not translating and reviewing this material increases the risk that the FBI will not detect information that may be important to its counterterrorism and counterintelligence efforts.

The FBI stated in response to our report that our audit reflects a reduction in the FBI's counterterrorism audio backlog from March 2005 through September 2008. However, we note that this statement is accurate only if the consideration of audio data is limited to data from one of several collection systems used by the FBI to collect counterterrorism audio material. Our audit explains that when the FBI considers data from this one collection system only, it is

presenting an incomplete picture of the translation backlog by failing to include important data on material collected outside this system.

We also concluded that the FBI cannot accurately determine the amount of foreign language material it collects because it lacks a consolidated collection and statistical reporting and evaluation system. While the FBI is developing such a system, in the interim it relies on its field offices to manually report workload data, and we found that this reported data was inconsistent with foreign language workload figures that were reported to executive management.

In response to a recommendation in our 2004 audit the FBI has improved its quality control over foreign language translations by creating a unit dedicated to quality control of FBI translations and by establishing a tracking system capable of monitoring compliance with quality control guidelines. However, we identified continued deficiencies in the management and oversight of the quality control process, such as not ensuring that FBI linguists and Certified Quality Control Reviewers were performing translations and quality control reviews only in languages in which they were certified.

Our audit also analyzed the FBI's progress in hiring linguists. We found that since our 2005 audit the number of linguists performing translations for the FBI has decreased from 1,338 in March 2005 to 1,298 in September 2008. As in our previous audits, we found that the FBI failed to achieve the linguist hiring goals for languages it identified as critical to FBI operations. For example, in FY 2008, the FBI only met its hiring target for 2 of the 14 critical languages for which it set goals. The FBI's inability to meet its hiring goals affects its ability to translate all of its collected material and hampers its efforts to reduce the backlog of unreviewed material, including material for its highest priority cases.

As we found in our previous audits, the FBI's process to hire linguists remains slow. We determined that from FYs 2005 through 2008 it took the FBI approximately 19 months to hire a contract linguist, an increase from the 16 months we found in our 2005 audit. Similar to our previous audits, the security clearance adjudication processes and proficiency testing accounted for the longest periods of time in applicant processing.

The OIG made 24 recommendations to help the FBI improve its management of its foreign language translation program and its ability to accurately and timely review audio, text, and electronic materials collected for its counterterrorism, counterintelligence, and criminal investigative operations. The FBI agreed with all the recommendations.

**DOJ's Efforts to Prevent Staff Sexual Abuse of Federal Inmates**

In September 2009, the OIG released a report examining the Department of Justice's (DOJ) efforts to prevent staff sexual abuse of inmates in federal prisons. Our review found that while DOJ's progress in implementing staff sexual abuse prevention programs has improved since 2001, DOJ needs to take additional steps to effectively deter, detect, investigate, and prosecute staff sexual abuse of federal prisoners.

It is a crime for a prison employee to engage in sexual contact or sexual relations with a federal prisoner, and consent by a prisoner is never a legal defense. Staff sexual abuse of prisoners has severe consequences for victims, undermines the safety and security of prisons, and in some cases leads to other crimes. For example, federal correctional workers who are sexually

involved with prisoners have been subject to extortion demands and may be more easily pressured to violate other prison rules and federal laws. Compromised personnel who have sexually abused prisoners also have been found to have provided contraband to prisoners, accepted bribes, lied to federal investigators, and committed other serious crimes in an effort to conceal their sexual involvement with federal prisoners.

In April 2005, the OIG issued a report concluding that the penalties under federal law for staff sexual abuse of federal prisoners without the use of threat or force were too lenient and resulted in U.S. Attorneys declining to prosecute many cases. In 2006, Congress passed two laws which made staff sexual acts and contact with a prisoner felonies with mandatory sex offender registration.

The OIG conducted this review to assess the Department's efforts to deter staff sexual abuse of federal prisoners. Our review covered fiscal years (FY) 2001 through 2008. Our review also analyzed the effect of legislation passed in 2006 on prosecutions of criminal sexual abuse cases and prison sentences for convicted staff sexual abusers.

We found that although the Federal Bureau of Prisons (BOP) has an established program for preventing and responding to allegations of staff sexual abuse, allegations of sexual abuse nevertheless doubled from FY 2001 through FY 2008. BOP officials told us they believe this increase is due to the BOP's efforts during this period to educate and encourage staff and inmates to report such abuse.

We identified several issues with the BOP's implementation of its program to prevent sexual abuse of inmates. For example, BOP officials at some prisons – in an effort to protect alleged inmate victims – automatically isolate and segregate the victims and subsequently transfer them to another federal prison without first considering less restrictive options for safeguarding them from further harm. Inmates often view those actions as punitive and, as a result, may be reluctant to report their sexual abuse or to cooperate with investigators. Additionally, BOP officials could not verify that all alleged inmate victims of staff sexual abuse had received appropriate victim services, such as psychological assessments and medical treatment. The OIG review also identified improvements that should be made in staff training, inmate education, and program oversight.

Due to the many challenges that staff sexual abuse and sexual misconduct investigations pose, such as lack of physical evidence, delayed reporting, and difficulty developing further evidence without exposing the inmate to further abuse, we found that the majority of staff sexual abuse allegations investigated by the BOP, OIG, and FBI do no not conclusively establish whether or not the alleged abuse occurred.

Since 2006 when the law changed misdemeanor sexual abuse crimes to felony crimes, the percentage of cases accepted for prosecution has increased from 37 percent under the old law to 49 percent under the new law. However, some prosecutors we interviewed continued to express a general reluctance to prosecute these cases. We also found that the prosecutors who accepted these cases had a very high success rate, with all but 7 of the 90 prosecutions resolved during the period of our review resulting in a conviction. We concluded that training federal prosecutors on the detrimental impact of staff sexual abuse on the inmates, on other prison staff, and on prison security would improve the Department's effectiveness in prosecuting these cases.

We also found that the stricter penalties for staff sex crimes enacted in 2006 had a mixed effect on the sentences of convicted defendants. While the number of defendants convicted of sexual abuse that received prison time increased after the changes, the legislation generally has not resulted in lengthier prison sentences. Further, we found that female staff members are less likely than male staff members to receive prison sentences when convicted of sexual abuse, and females who were convicted received shorter sentences than their male colleagues. While female staff members comprised about 25 percent of the BOP workforce in each year of the study period, they were the subjects in 30 – 39 percent of the allegations of staff sexual abuse and sexual misconduct.

Our review also examined the actions of the U.S. Marshals Service (USMS) to prevent sexual abuse of detainees in its custody. We found that the USMS has not established a sexual abuse prevention program to prevent, detect, or investigate staff sexual abuse in its cellblocks and transportation system. While USMS officials said they believe the agency's general policies for protecting prisoners and USMS personnel are adequate to protect against staff sexual abuse, we concluded that the USMS policies do not provide sufficient guidance and recommended that the USMS develop new policies to specifically address this issue.

The OIG made 21 recommendations to improve DOJ's efforts to prevent, detect, and respond to staff sexual abuse as well as to better investigate, discipline, and prosecute federal personnel that sexually abuse inmates. The BOP agreed with all but two of the recommendations to improve its sexual abuse prevention program.

**DOJ's Involvement with the President's Surveillance Program**

In the weeks following the terrorist attacks of September 11, 2001, the President authorized National Security Agency (NSA) to conduct a classified program to detect and prevent further attacks in the United States. The program was reauthorized by the President every 45 days with certain modifications. Collectively, the activities carried out under these Authorizations are referred to as the "President's Surveillance Program" ("PSP" or "Program").

In July 2009, the OIG completed a 407-page classified report, entitled "A Review of the Department of Justice's Involvement with the President's Surveillance Program," detailing the Department's role in the PSP. The report examined the Department's controls over and use of information related to the PSP and the Department's compliance with legal requirements governing the PSP. The OIG focused in particular on the Department's role in providing legal advice concerning the Program and on the FBI's role as a consumer of information from the Program. The OIG found that only one Office of Legal Counsel (OLC) attorney, Deputy Assistant Attorney General John Yoo, was read into the PSP during its first year and a half of operation. Other Department officials who were later read into the PSP became concerned about the factual and legal basis for Yoo's legal memoranda and conducted a comprehensive reassessment of the legal basis for the PSP.

The OIG concluded that it was extraordinary and inappropriate that a single DOJ attorney was relied upon to conduct the initial legal assessment of the PSP, and that the lack of oversight and review of Yoo's work, as customarily is the practice of OLC, contributed to a legal analysis of the PSP that at a minimum was factually flawed. Deficiencies in the legal memoranda became apparent once additional DOJ attorneys were read into the program in 2003 and when those attorneys sought a greater understanding of the PSP's operation. The OIG concluded that the

strict controls over DOJ access to the PSP undermined DOJ's ability to perform its critical legal function during the PSP's early phase of operation.

The OIG also sought as part of its review to assess the role of PSP-derived information and its value to the FBI's overall counterterrorism efforts. FBI Director Mueller stated that he believes the PSP was useful, and he based this conclusion in part on the results of a survey the FBI conducted in 2006 to assess the impact of PSP-derived information.

The OIG also interviewed FBI officials, agents, and analysts responsible for handling PSP information about their experiences with the program. These assessments generally were supportive of the program as "one tool of many" in the FBI's anti-terrorism efforts that "could help move cases forward," although most PSP leads were determined not to have any connection to terrorism. The OIG also examined several cases that have frequently been cited as examples of the PSP's contribution to the Intelligence Community's counterterrorism efforts.

However, the OIG also found that the exceptionally compartmented nature of the program created some frustration for FBI personnel. Some agents and analysts criticized the PSP-derived information they received for providing insufficient details, and the agents who managed counterterrorism programs at the FBI field offices the OIG visited said the FBI's process for disseminating PSP-derived information failed to adequately prioritize the information for investigation.

In sum, the OIG found it difficult to assess or quantify the overall effectiveness of the PSP program as it relates to the FBI's counterterrorism activities. However, based on the interviews conducted and documents reviewed, the OIG concluded that although PSP-derived information had value in some counterterrorism investigations, it generally played a limited role in the FBI's overall counterterrorism efforts.

The OIG also considered public statements by former Attorney General Alberto Gonzales about the Program. Aspects of the PSP were first disclosed publicly in a series of articles in The New York Times in December 2005. Subsequently, Attorney General Gonzales was questioned about NSA surveillance activities in two public hearings before the Senate Judiciary Committee in February 2006 and July 2007. As part of its review, the OIG examined whether Gonzales made false, inaccurate, or misleading statements to Congress in those hearings while testifying about a dispute between White House and Department officials in March 2004 concerning the PSP. The OIG concluded that Gonzales did not intend to mislead Congress, but found that his testimony was confusing, inaccurate, and had the effect of misleading those who were not knowledgeable about the Program.

Title III of the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FISA Amendments Act) required the Inspectors General of Intelligence Community agencies that participated in the PSP to conduct a comprehensive review of the program. The Department of Justice OIG, worked with the Inspectors General of the Department of Defense, Central Intelligence Agency, National Security Agency, and the Office of the Director of National Intelligence, to conduct the review required under the FISA Amendments Act. On July 10, 2009, the group submitted to the Senate and House Intelligence and Judiciary Committees five classified reports from the OIGs of the individual agencies participating in the Program, a classified summary of the OIGs' reviews, and an unclassified report summarizing the portions of

the collective results of the OIG reviews that could be released in unclassified form. The unclassified summary is available on the OIG's public web site.

**The FBI's Terrorist Watchlist Nomination Process**

In May 2009, the OIG issued an audit report examining the FBI's practices for nominating known or suspected terrorists to the consolidated terrorist watchlist and determined that the FBI failed to nominate subjects, did not nominate many others in a timely fashion, and did not update or remove certain watchlist records as required.

As a follow-up to our March 2008 report, which examined the Department's processes for nominating known or suspected terrorists to the consolidated terrorist watchlist, we found that 15 percent of the FBI terrorism investigations we reviewed failed to nominate terrorism subjects to the consolidated terrorist watchlist. We also found that 78 percent of the watchlist nominations reviewed were not processed within the FBI's time standards, typically up to 20 calendar days. Instead, the FBI's untimely nominations took an average of 42 days to process. In addition, the FBI failed to modify the nomination records to include identifying information it obtained after the initial nomination was processed.

Because the consolidated terrorist watchlist is used by government frontline screening personnel to determine how to respond when a known or suspected terrorist requests entry into the United States, the failure either to place appropriate individuals on the watchlist or place them on the watchlist in a timely manner increases the risk that these individuals can enter and move freely within the United States. In fact, we determined that 12 of the terrorism subjects we reviewed who either were not watchlisted or were watchlisted in an untimely manner may have traveled into or out of the United States during the time period they were not watchlisted.

Despite FBI policy that generally requires agents to remove subjects' watchlist records when the FBI investigation is closed, we found that the FBI failed to remove 7 subjects and did not timely remove another 61 subjects from the 85 closed terrorism investigations we reviewed. Failure to remove or timely remove individuals could lead to the denial of a passport or visa, boarding a flight, or entry into the United States or cause the individual to be unnecessarily questioned.

Another finding related to the FBI, on behalf of the Department of Defense (DOD), nominating about 64,000 individuals detained by the U.S. military or individuals considered by foreign governments as known or suspected terrorists since 2001. These nominations were made outside of established FBI internal controls designed to ensure that FBI-nominated watchlist records are complete and accurate. We found that many of these records were supported by limited information linking the individual to terrorism. Following our inquiries, in October 2008 the FBI halted the practice of handling DOD watchlist nominations.

The OIG also found that 35 percent of the approximately 68,000 identities sourced to the FBI in the consolidated terrorist watchlist were sourced to old or non-terrorism FBI investigation classifications. The OIG analyzed a sample of 164 of the watchlisted individuals related to these identities and found that 94 of them should have either been removed from the watchlist previously or the FBI could no longer support their inclusion. A further analysis of 59 of these individuals found that they had been improperly maintained on the watchlist by the FBI for an average of 1,112 days.

In response to our audit, the FBI has begun taking corrective actions, such as providing training to terrorism case agents and establishing dedicated watchlist coordinator positions in FBI field offices. However, we believe that weaknesses still exist. The OIG made 16 recommendations to the FBI regarding nominations to, modifications of, and removal of identities from the consolidated terrorist watchlist. The FBI agreed with our recommendations.

**DOJ's Management of the Federal Employees' Compensation Act Program**

In August 2009, the OIG released a report examining the Department's management of claims submitted by DOJ employees under the Federal Employees' Compensation Act (FECA) program. Our audit concluded that DOJ lacks effective controls to reduce the risk of waste, fraud, and abuse in its FECA program, and to ensure that employees return to work when appropriate.

The FECA program, which is primarily administered by the Department of Labor's Office of Workers' Compensation Programs, provides medical benefits, income replacement, and certain support services to non-military employees of the federal government with work-related illnesses or injuries, or in the case of death, survivor benefits to family members. However, each federal agency, including DOJ, has financial and management responsibilities for FECA cases filed by its own employees. Our audit focused on the five components that encompass 95 percent of DOJ's FECA costs: the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), Federal Bureau of Prisons (BOP), Drug Enforcement Administration (DEA), Federal Bureau of Investigation (FBI), and the U.S. Marshals Service (USMS).

We found that in comparison to other agencies, DOJ had relatively high rates of injury, with an average rate of 4.53 injuries per 100 employees from fiscal years (FY) 2005 to 2008. This is the fourth highest rate of injury out of 29 major federal agencies. In addition, DOJ's overall benefit expense of $102 million for FY 2008 ranked seventh out of the 29 agencies.

Our audit determined that with the exception of the BOP and FBI, the DOJ components we audited were generally reactive rather than proactive in their monitoring of FECA cases. In addition, DOJ components did not maintain all of the information necessary to effectively manage employees' FECA cases. For 15 percent of the cases we selected for review, no case file was maintained. The DEA was missing the largest percentage (48 percent) of case files; in contrast the BOP maintained all case files we selected for review. Our audit also found that 21 percent of the case files we reviewed were missing claim forms substantiating the work-related injury, 73 percent lacked evidence of a second medical opinion, and 34 percent lacked evidence of medical updates necessary to monitor an employee's condition in order to return the employee to work when appropriate.

In addition, we determined that DOJ's weaknesses in monitoring FECA cases has resulted in a substantial amount of money that continues to be paid to employees who have remained on long-term disability without a review as to whether their current medical condition entitles them to remain on disability. The long-term cases where the claimant remained on disability for over 3 years comprised only 6 percent of the total number of DOJ's FECA cases but accounted for over $153 million (or 54 percent) of DOJ's total FECA expenses from 2006 through 2008. Overall, DOJ's FECA expense increased an average of $6.4 million per year, which was the third highest annual increase in the federal government since FY 2000.

The OIG made five recommendations to help improve the management of DOJ's FECA program, including implementing procedures to ensure that FECA cases are periodically reviewed, obtaining periodic medical updates and second medical opinions when necessary, and evaluating FECA cases for return to work opportunities or light duty assignments. DOJ concurred with the recommendations.

**Civil Division's Laptop Encryption Program**

In July 2009, the OIG issued an audit examining the Civil Division's Laptop Encryption Program and Practices. The audit included laptop computers owned by the Civil Division and laptop computers owned by contractors, subcontractors, and other vendors working for the Civil Division. For the laptop computers owned by the Civil Division, the OIG audit found that the Civil Division has complied with DOJ requirements by ensuring that its own laptop computers are encrypted to protect DOJ data. For the laptop computers owned by Civil Division contractors, subcontractors, and vendors, the OIG audit found that the Civil Division's efforts to ensure contractor safeguards over DOJ data need significant improvement. We found that: (1) an inventory of non-Civil Division laptop computers was not maintained; (2) a large percentage of contractor laptops used to process DOJ data were not encrypted; and (3) contractors had not received notification of DOJ laptop encryption requirements.

Civil Division officials stated that some of their contractors regard their participation in Civil Division cases as a public service and that these experts are not necessarily proficient in technology, nor do they have information technology staffs on which to rely. In our judgment, given the sensitive nature of the litigation work performed by the Civil Division, Civil Division contractors, subcontractors, and venders should encrypt their laptop computers or exclusively use Civil Division-owned laptop computers. The OIG made seven recommendations to the Civil Division to enhance its safeguards over DOJ data on laptop computers. The Civil Division concurred with all seven recommendations.

**DOJ's Use of Less Lethal Weapons**

In May 2009, the OIG released a report that examined the Department's use of less-lethal weapons, such as batons, pepper spray, and conducted energy devices such as Tasers. While our review found that the Department's law enforcement components are expanding their use of less-lethal weapons, the Department does not have a specific policy to govern the use by its own employees or by state and local law enforcement personnel serving on Department task forces.

All five of the Department's law enforcement components (FBI, ATF, DEA, USMS, and BOP) authorize and train some of their personnel to use specific less-lethal weapons. For example, FBI and DEA Special Agents are only authorized to use batons and pepper spray, while the DEA, USMS, and BOP are authorized to use batons, pepper spray, "bean bag" shotgun rounds, and some form of a conducted energy device. The OIG found that the use of less-lethal weapons varies widely by component: the DEA reported no use; the FBI reported limited use; ATF and USMS statistics reported moderate but increasing use; and the BOP's data showed the most use. There have been no reported fatalities or significant injuries resulting from the use of less-lethal weapons by Department components during the past 5 years. However, fatalities have occurred at the state and local level, particularly following the use of Tasers or similar conducted energy devices.

Without a specific Department policy regarding the use of less-lethal weapons, components have developed individual policies to guide their personnel in the use of these weapons. However, the individual policies do not always address the use of these weapons by state and local task force members. For example, the FBI and DEA do not have policies that address the use of Tasers by state and local members of their task forces, while the USMS does not mandate that state and local task force officers abide by its less-lethal weapons policies, including its Taser policy.

Although ATF, the BOP, and the USMS have obtained new types of less-lethal weapons in the last several years, the OIG found no coordinated Department-wide assessment of new less-lethal weapon technologies or development of use policies and training materials. Our review also found that the components were not aware of work done elsewhere in the Department, including studies funded by the National Institute for Justice (NIJ), which assessed new less-lethal technologies, and investigations by the Civil Rights Division, which yielded detailed information about law enforcement policies and practices involving their use of less-lethal weapons at the state and local levels.

The OIG made four recommendations, including for the Department to coordinate the development of a Department-wide policy addressing the use of less-lethal weapons and ensure that its law enforcement components periodically analyze their use of less-lethal weapons and assess emerging trends in the use of such weapons.

**Review of the FBI's Disciplinary System**

In May 2009, the OIG released a report examining whether the FBI has imposed consistent, reasonable, and timely discipline on employees found to have committed misconduct. The OIG previously conducted similar reviews of disciplinary systems in four other components. We found that aspects of the FBI's disciplinary system worked well, and the FBI improved timeliness in each phase of its disciplinary process. However, deficiencies still existed that hampered the FBI's ability to ensure reasonable and consistent discipline. We also found that concerns remained about a double standard of discipline for higher-ranking FBI employees.

During our review, we determined that potential misconduct was not consistently reported to FBI headquarters or to the OIG, as required by FBI policy. We also found that disciplinary decisions generally were reasonable, but some of the decisions on what penalties to impose contained inconsistencies that could not be explained by the record in the case files. In addition, we found a lack of clear guidance about the appropriate standard of review that appellate officials should apply when reviewing penalties imposed by the FBI's Office of Professional Responsibility (OPR).

With regard to the issue of a double standard of discipline, a third of the FBI employees we surveyed believed a double standard existed for higher-ranking employees. Disciplinary outcomes showed that misconduct allegations against senior executive service (SES) employees were more likely to be unsubstantiated (49 percent) than those against non-SES employees (22 percent). More significantly, penalties imposed on SES employees for misconduct were mitigated on appeal much more frequently than for non-SES employees. We found that appellate officials often substituted their judgment for FBI OPR's decisions, even on findings of fact, and FBI appellate officials unreasonably mitigated discipline in most of the SES cases.

While reviewing the FBI's discipline process, we found that FBI employees with imposed suspensions frequently did not serve their sentence or served for the incorrect length of time. In addition, the FBI's practice of beginning all suspensions at the close of business on Fridays, unlike other Department law enforcement components, resulted in FBI employees effectively serving fewer days and receiving less time off without pay than employees elsewhere in the Department.

We made 16 recommendations to help the FBI improve its disciplinary system, including reminding FBI employees to report misconduct to FBI headquarters or the OIG, requiring FBI OPR to better document in the case files the information it considers when making decisions, considering the appointment of a permanent appeals decision maker or board, ensuring that FBI policies are applied consistently to all levels of employees at all stages of the disciplinary process, and reviewing the files of all employees suspended since October 2004 to ensure that they served their suspensions. The FBI concurred with our recommendations and is taking steps to implement them.

**Procedures Used by the OJJDP to Award Discretionary Grants in FY 2007 and Report of Investigation Relating to a Former Administrator of OJJDP**

In April 2009, the OIG released an audit report and an investigative report examining how the Office of Juvenile Justice and Delinquency Prevention (OJJDP) awarded over $113 million in discretionary grants in fiscal year (FY) 2007. The OIG audit and investigation also reviewed allegations that former OJJDP Administrator J. Robert Flores improperly awarded grants and contracts.

Prior to FY 2007, Congress had earmarked almost all of OJJDP's grant funds. Because the Department's FY 2007 appropriation was discretionary rather than earmarked and was passed well after the fiscal year began, both the Office of Justice Programs (OJP) and OJJDP struggled with how to award the grant funds on an expedited timeframe.

Our audit found that then-OJP Assistant Attorney General Regina B. Schofield allocated $74 million of the $113 million for OJJDP noncompetitive grants or "invitational awards" to 17 organizations, many of whom had received earmarks in the past, leaving about $40 million for competitive awards. While Schofield and other OJP officials said they only gave invitational awards to organizations that had demonstrated a strong record of performance and result, they could not provide us with any documents showing that it made merit-based assessments for these invitational grants.

With respect to the grants competitively awarded by OJJDP, we found that Flores recommended awards to several organizations, including the World Golf Foundation, the Best Friends Foundation, and Victory Outreach, whose proposals received peer review scores that were lower than applications submitted by other organizations that did not receive award recommendations. Schofield subsequently approved Flores's award recommendations. We concluded that OJP and OJJDP decision makers should have justified and documented the rationale for award recommendations that deviated significantly from peer review results.

Moreover, as described in the OIG investigative report, OIG investigators determined that Flores violated federal ethics regulation by accepting a round of golf valued at $159 from World Golf

officials when World Golf's First Tee Initiative was an OJJDP grantee. Flores did not reimburse World Golf for the round of golf until the day before he testified before a congressional oversight committee, which was 2 years after accepting the golf game and about a year after he had recommended World Golf for a grant award in FY 2007.

In addition, the OIG report of investigation found that Flores circumvented federal acquisition regulations by hiring a consultant through a non-competitive contract and was not sufficiently sensitive to potential conflict of interest issues arising in another contract.

The OIG audit made ten recommendations to help OJP and OJJDP better administer its grant programs.

**The Department's Litigation Case Management System**

In March 2009, the OIG released a report examining the Department's progress toward developing a Department-wide Litigation Case Management System (LCMS). Our audit concluded that the LCMS project, which the Department began in 2004, is more than 2 years behind schedule, approximately $20 million over budget, and at significant risk of not meeting the Department's requirements for litigation case management.

Each of the Department's litigating divisions maintains their own case management system, and these individual systems are unable to share information with other Department case management systems. The Department began the LCMS project to develop an information technology (IT) infrastructure for effectively storing case information once, managing it centrally, and making it available to the approximately 14,500 authorized users in the Department's seven litigating divisions.

DOJ initially estimated the LCMS would be implemented in the EOUSA and USAOs by March 2008, with implementation in the six other litigating divisions by December 2010. DOJ now estimates that the LCMS will not be fully implemented in EOUSA and USAOs until July 2010, more than 2 years later than estimated and only 5 months before the initial estimated completion date for all seven litigating divisions. DOJ also initially estimated that the primary contract to develop and implement the system would cost approximately $42 million, of which about $35 million was for implementation of the LCMS in EOUSA and USAOs. However, as of January 2009 the Department estimated the cost of implementing the LCMS in EOUSA and USAOs at about $61 million, 75 percent higher than the initial estimate and $18 million more than the initial estimated cost of implementing the LCMS in all seven litigating divisions.

Because implementation of the LCMS in EOUSA and USAOs is significantly behind schedule and over budget, the Department has postponed any further work related to the other litigating divisions and does not have current schedule and cost estimates for completing the LCMS in the other divisions. Moreover, we found that officials in the remaining six litigating divisions are uncertain that the LCMS will meet their needs.

The OIG review found that causes for the delays and budget overruns included: 1) the requirements planning process was not effective, and requirements were modified and added after significant work had been done; 2) system integration and user acceptance testing revealed severe defects, including data migration errors, access restrictions, and other errors that required

an extensive amount of time to correct; and 3) the Department's oversight efforts identified severe difficulties the contractor was having meeting the schedule and cost requirements, but the Department's actions did not minimize the schedule and cost overruns.

We concluded that both the Department and the contractor share responsibility for the significant delays and budget overruns in this project. We recommended that the Department's Chief Information Officer reevaluate the viability of implementing the LCMS in the other litigating divisions. The Department agreed with our recommendation.

**The Convicted Offender DNA Backlog Reduction Program**

In March 2009, the OIG issued a report examining OJP's Convicted Offender DNA Backlog Reduction Program (Backlog Reduction Program), a grant program that provides funding to help states reduce the backlog of convicted offender DNA samples. Our audit found that the Backlog Reduction Program has contributed to the decrease in the nationwide backlog of DNA samples awaiting analysis, but the Department could increase the effectiveness of the program by improving its method for collecting information from grantees, by ensuring that grants are used in a timely manner, and by not awarding funds to grantees who have not utilized prior awarded program funds.

In 2004, the Department implemented a 5-year, $1 billion DNA grant program initiative to improve the capacity of law enforcement agencies to solve crimes using DNA evidence. As part of this DNA initiative, the Department provided funding to help states reduce the backlog of convicted offender samples awaiting analysis and entry into the FBI's Combined DNA Index System (CODIS).

Between FYs 2005 and 2007, 39 states received Backlog Reduction Program grants totaling $41.3 million to analyze 1.46 million DNA samples either through in-house analysis or by sending samples to approved vendor laboratories. We concluded that the national backlog of convicted offender DNA samples has been reduced significantly as a result of efforts by the states to analyze convicted offender DNA samples. However, the backlog may continue to grow because of recent legislation in some states that increased the number of offenses for which DNA samples could be collected.

We found several areas where the Backlog Reduction Program could be improved. Despite the fact that the Department required state laboratories to collect information on performance measures, the Department did not provide adequate guidance to state laboratories on collecting and reporting performance and did not adequately use the information reported by the state laboratories to manage its Backlog Reduction Program. As a result, we identified inconsistencies with the statistical information reported by the laboratories, which prevents the Department from fully and accurately assessing overall Backlog Reduction Program performance.

We also found significant delays to the start of several Backlog Reduction Program awards, which caused more than 180,000 convicted offender DNA samples to not be uploaded to CODIS in a timely manner. These Backlog Reduction Program awards lacked any indication of activity in both financial and programmatic reports submitted to the Department, suggesting that award recipients may have encountered problems fulfilling the award requirements or that the Backlog Reduction Program may not be meeting the specific needs of the award recipient.

In addition, we found that the Department continued to award funding to several state laboratories that had not utilized previous award funding, despite the fact that the Department added requirements to the FY 2008 Backlog Reduction Program solicitation to reject applications from laboratories with prior awards that remain entirely unobligated as of the posting date of the solicitation. Awarding additional funding to state laboratories with inactive awards prevents those funds from being put to better use by another laboratory or federal program.

The OIG made 11 recommendations to help strengthen the Department's oversight and administration of the Backlog Reduction Program. The Department agreed with our recommendations.

## Examples of Recent Investigations Division Cases

### Obstruction of Justice & Related Civil Rights Violations

An investigation by the OIG's Chicago Field Office led to the arrest of DEA special agent pursuant to an indictment returned in the Northern District of Ohio, charging him with seven counts of obstruction of justice, one count of false statements, seven counts of perjury and three counts of violating individuals' civil rights. In addition, a Richland County, Ohio sheriff's detective was arrested and pled guilty in the Northern District of Ohio to depriving an individual's civil rights. The OIG investigation determined that the DEA special agent intentionally framed 17 individuals during the course of 13 controlled drug buys carried out in Mansfield, Ohio, and that the sheriff's detective participated in framing one of those individuals. The DEA special agent allegedly placed false statements in his reports of drug transactions, suppressed evidence favorable to an accused from prosecutors and the courts, and perjured himself before the District Court at a detention hearing and the two trials that ensued from the investigation. 12 of the 17 individuals framed by the DEA special agent were collectively sentenced to 70 years in prison before their convictions were dismissed or overturned, and one individual served 16 months of a 10 year sentence before being exonerated. The sheriff's detective admitted to providing false testimony at the narcotics trial of one of the 17 individuals.

### Murder

An investigation by the OIG's New York Field Office resulted in the conviction of former FBI Special Agent John Connolly on charges of second-degree murder in connection with the 1982 shooting death of a gambling executive and the murder of two other FBI Boston informants. Connolly was indicted on May 4, 2005, on charges of first degree murder and conspiracy to commit murder in relation to the killing of former World Jai Alai president John Callahan in 1982. A joint investigation by the OIG's Boston Area Office, the U.S. Attorney's Office for the District of Massachusetts, the DEA, the Massachusetts State Police, the Miami-Dade Police Department, and the Miami-Dade State Attorney's Office developed evidence that while employed by the FBI in Boston, Connolly assisted the criminal activities of the Winter Hill Gang led by James "Whitey" Bulger, by supplying gang members with sensitive law enforcement information and intelligence that led directly to the murder of Callahan. Connolly is currently serving a 10-year sentence in federal prison for racketeering, obstruction of justice, and other charges stemming from his role in protecting members of the Winter Hill Gang while simultaneously using them as FBI informants. Connolly received an additional sentence of 40 years in prison for the second-degree murder conviction.

### Solicitation of Attempted Murder

An investigation by the OIG's Miami Field Office led to the arrest of a BOP inmate incarcerated at the Federal Correctional Complex (FCC) in Coleman, Florida, on charges of (1) attempting to kill an OIG special agent, (2) attempting to kill another person in retaliation for providing information to law enforcement, (3) attempting to injure yet another person in retaliation for appearing as a witness, and (4) using the mail and a facility in interstate commerce in connection with murder for hire. The inmate, formerly a BOP Correctional Officer in Danbury, Connecticut, previously was convicted and sentenced to 15 years' incarceration for sexual abuse of a female ward and plotting with a female inmate to murder his wife. This original case was investigated by the OIG's New York Field Office. Shortly after beginning his sentence in FCC Coleman, the former correctional officer solicited assistance from inmates to murder his now estranged wife, her current boyfriend, the female inmate from the previous investigation, and the

OIG Special Agent who investigated the original case. In an investigation by the OIG's Miami Field Office, the former correctional officer provided an OIG undercover agent with physical descriptions of each victim, their geographical locations, specific instructions as to what he wanted done, and an initial payment of $500 for the murders from his BOP inmate account. Judicial proceedings continue.

**Bribery**

An investigation by the OIG's Miami Field Office led to the arrest, guilty plea and sentencing of a BOP correctional officer assigned to the Federal Correctional Institution, in Jesup, Georgia. The OIG investigation determined that the correctional officer accepted $5,800 in bribes in exchange for the introduction of marijuana, cell phones, and cigarettes to inmates. The correctional officer was sentenced in the Southern District of Georgia to 30 months' incarceration followed by 36 months' supervised release. He also resigned from the BOP as a result of our investigation.

**Embezzlement**

An investigation by the OIG's Miami Field Office led to the arrest of a DEA special agent on charges of converting the property of another, embezzlement of public funds, and money laundering. An indictment returned in the Northern District of Georgia alleged that the special agent, who served as a team leader and evidence custodian at the DEA's Atlanta Airport Task Force, over a 2-year period, embezzled cash seized from money couriers for drug organizations by instructing local police officers to turn over seized money to him without counting it. The special agent allegedly stole more than $200,000, and used a portion of the embezzled money to build a custom home in Orlando, Florida. He was sentenced to 21 months' incarceration followed by 12 months' supervised release and was ordered to perform 100 hours community service and to pay $92,614 in restitution. As part of the plea agreement, the DEA special agent is banned from ever seeking employment in federal, state, or local law enforcement.

A separate investigation by the OIG's Chicago Field Office led to the arrest of an FBI financial manager on charges of embezzlement of government funds. The investigation determined that the financial manager stole $22,425 designated for undercover operations. She also falsified receipts to make it appear that invoices were paid, but instead deposited the money into her own bank accounts. The financial manager pled guilty and was sentenced to 6 months' home confinement and 36 months' supervised release. She also was ordered to pay restitution to the FBI in the amount of $86,025. The financial manager resigned her position as a result of our investigation

**Misuse of Grant Funds and False Claims**

An investigation by the OIG's Fraud Detection Office found that the City of Macon misspent approximately $350,000 of a $900,000 Safe Schools Initiative earmark grant from the Office of Juvenile Justice and Delinquency Prevention, which was intended to provide services for at-risk youth. Approximately $71,000 of the City of Macon's $350,000 in expenditures was unallowable (e.g., travel, food purchases, cosmetic office enhancements, supplies, and equipment) per federal grant rules and regulations and documentation did not exist to support an estimated $279,000 in expenditures. Additionally, every quarterly financial status report submitted to the Office of Justice Programs was false. In lieu of a civil complaint being filed, the U.S. Attorney's Office for the Middle District of Georgia reached a civil settlement with the City

of Macon for $315,002.09. If the City of Macon fails to make the payments, then the U.S. Attorney's Office will file a civil action in court.

A separate investigation resulted in the Northeastern Massachusetts Law Enforcement Council (NMLEC) agreeing to pay $200,000 to settle allegations related to civil false claims in connection with a DOJ grant program. The NMLEC is a non-profit consortium of 49 Boston Area police departments and this settlement was based on their financial inability to pay a higher sum. An investigation led by the OIG's Fraud Detection Office, with the assistance of the OIG's Boston Area Office and the FBI determined that on June 16, 2003, the NMLEC used DOJ grant funds to write a check to a grant consultant with Crest Associates, for $832,395. The purpose of this check was to represent to the government that all awarded funds had been spent within the required program timelines. The grant consultant subsequently used these funds to make purchases or provide services on behalf of NMLEC programs. However, as much as $303,000 could not be properly supported. The grant consultant committed suicide during this investigation.

**Theft and Money Laundering**

A joint investigation by the OIG's Denver Field Office, the FBI, and the Internal Revenue Service Criminal Investigation Division resulted in the arrest and plea of a DOJ grantee to charges of making false statements, theft from an Indian tribal government receiving federal funds, and money laundering. The investigation determined that he grantee, in her position as President of the San Juan Southern Paiute Tribe, obtained federal funds from several agencies, including a Community Oriented Policing Services (COPS) grant totaling $224,997 to hire three police officers. The grantee failed to hire the three police officers, and instead submitted a false record to COPS stating that she had. She converted the stolen funds for her own use. The grantee was sentenced to 24 months' incarceration followed by 36 months of supervised release and fined $75,000.

**Misuse of Position by USMS Attorney**

The OIG investigated allegations that U.S. Marshal Service (USMS) attorney Joseph Band misused his official position by requesting and using USMS resources while engaging in his personal employment. Our investigation revealed that when Band attended sporting events as a paid, part-time statistician for Fox Sports, he asked for and received transportation in USMS cars, driven by Deputy U.S. Marshals (DUSM), to and from the games. We concluded that Band's conduct violated USMS standards of ethical conduct for misuse of position and USMS policy on the proper use of government vehicles. We also concluded that three U.S. Marshals inappropriately approved Band's requests to use USMS resources for his personal business.

Our January 2009 report was provided to the U.S. Attorneys Offices in Boston and the Eastern District of Virginia, both of which declined criminal prosecution in this matter. We also provided our report to the USMS for appropriate action along with recommendations for the USMS to address weaknesses in its internal controls regarding its policies on outside employment. The USMS has agreed to implement our recommendations. Band retired from federal service at the conclusion of our investigation.

**Conspiracy to Distribute Cocaine**

A joint investigation by the OIG's Washington Field Office and the DEA resulted in the arrest of a Civil Division legal secretary on charges of conspiracy to distribute cocaine and possession

with intent to distribute cocaine. The joint investigation revealed that the legal secretary attempted to possess 500 grams of cocaine with intent to distribute. The U.S. Attorney's Office for the District of Maryland also is seeking the forfeiture of $250,000 that was seized from the legal secretary.

**Criminal Access of a Government Database**

An investigation by the OIG's New York Field Office led to the arrest and conviction of a former FBI supervisory special agent for criminally accessing a sensitive FBI database for personal purposes. The OIG's investigation determined that the former supervisory special agent improperly downloaded a copy of a confidential informant's FBI report that contained information relevant to a criminal case that was being actively prosecuted. The former supervisory special agent then provided a copy of the report to a personal acquaintance who, in turn provided a copy of the report to defense attorneys. The defense attorneys filed the FBI report in the criminal case to support an allegation that the United States was improperly withholding exculpatory information from the defense. Unbeknownst to the defense attorneys, the judge in the case had previously ruled, *ex parte*, that the information was not exculpatory to the defense. The former supervisory special agent consistently informed his supervisors that news stories connecting him to the case were false and also lied about his actions to OIG investigators. Because of the investigation, the former supervisory special agent resigned his position with the FBI. He was sentenced to 12 months' probation and ordered to perform 250 hours of community service and pay a $5,000 fine for criminally accessing a sensitive FBI database for personal purposes.

**Lying to a Federal Grand Jury**

An investigation by the OIG's New York Field Office resulted in the arrest and jury conviction of a Deputy U.S. Marshal (DUSM) on charges of providing a firearm and ammunition to a convicted felon and lying to a federal Grand Jury. The OIG investigation determined that the DUSM purchased a semi-automatic handgun by certifying on USMS letterhead that it was to be used for "official use" only and that he would not transfer it to anyone else. The DUSM later gave this weapon to a friend with an extensive criminal history, including aggravated assault, robbery, and unlawful possession of a handgun. Sentencing is pending.

**Criminal Invasion of Privacy**

An investigation by the OIG's Washington Field Office resulted in the arrest of two FBI police officers on charges of criminal invasion of privacy and conspiracy. The investigation found that the officers were working in an FBI security control room for a Criminal Justice Information Services office located in a shopping mall in West Virginia. While the officers were on duty, a local event was taking place in which high school girls could buy low-cost prom dresses. The FBI police officers manually manipulated the focus of an FBI security camera located in the mall's ceiling to view into the makeshift dressing room used by the students for the event. The recording taken by the camera showed girls changing in and out of prom dresses, including several girls who could be seen in their underwear and one girl who could be seen topless. One of the police officers pled guilty to a West Virginia state charge of conspiracy to commit criminal invasion of privacy. He was sentenced to six months' probation, fined $200, and ordered to repay court costs. The second police officer was sentenced to six months incarceration followed by one year of supervised release.

**PERFORMANCE AND RESOURCES TABLE (Goal 1)**

**Decision Unit:** OIG/Audits, Inspections, Investigations, and Reviews

**DOJ Strategic Plan:** Supporting the Mission: Efficiency and Integrity in the Department of Justice.

**OIG General Goal #1:** Detect and deter misconduct in programs and operations within or financed by the Department.

| WORKLOAD/RESOURCES | Final Target | | Actual | | Projected | | Changes | | Requested (Total) | |
|---|---|---|---|---|---|---|---|---|---|---|
| | FY 2009 | | FY 2009 | | FY 2010 | | Current Services Adjustment and FY 2011 Program Change | | FY 2011 Request | |
| **Total Costs and FTE** | FTE | $000 | FTE | $000 | FTE | $000 | FTE | $000 | FTE | $000 |
| (reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total) | 453 | $75,681 [$18,697] | 432 | $75,584 [$18,697] | 497 | $84,368 [$19,730] | 13 | $4,424 [$1,338] | 510 | $88,792 [$21,068] |
| **Performance Report and Performance Plan** | | | | | | | | | | |
| Number of Cases Opened per 1,000 DOJ employees: | | | | | | | | | | |
| Fraud | | ** | | 0.50 | | ** | | ** | | ** |
| Bribery | | ** | | 0.30 | | ** | | ** | | ** |
| Rights Violations | | ** | | 0.15 | | ** | | ** | | ** |
| Sexual Crimes | | ** | | 0.21 | | ** | | ** | | ** |
| Official Misconduct | | ** | | 1.28 | | ** | | ** | | ** |
| Theft | | ** | | 0.25 | | ** | | ** | | ** |
| **Workload** | | | | | | | | | | |
| Investigations closed | | 350 | | 367 | | 350 | | 2 | | 352 |
| Integrity Briefings/Presentations to DOJ employees | | 140 | | 346 | | 150 | | | | 150 |
| DOJ employees at Integrity Briefings | | 4,200 | | 7,545 | | 4,200 | | | | 4,200 |

## PERFORMANCE AND RESOURCES TABLE (Goal 1)

**Decision Unit:** OIG/Audits, Inspections, Investigations, and Reviews

**DOJ Strategic Plan:** Supporting the Mission: Efficiency and Integrity in the Department of Justice.

**OIG General Goal #1:** Detect and deter misconduct in programs and operations within or financed by the Department.

| WORKLOAD/RESOURCES | Final Target | | Actual | | Projected | | Changes | | Requested (Total) | |
|---|---|---|---|---|---|---|---|---|---|---|
| | FY 2009 | | FY 2009 | | FY 2010 | | Current Services Adjustment and FY 2011 Program Change | | FY 2011 Request | |
| **Total Costs and FTE** (reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total) | FTE 453 | $000 $75,682 [$18,697] | FTE 432 | $000 $75,584 [$18,697] | FTE 497 | $000 $84,368 [$19,730] | FTE 13 | $000 $4,424 [$1,338] | FTE 510 | $000 $88,792 [$21,064] |
| **Performance Report and Performance Plan** | | | | | | | | | | |
| **Intermediate Outcome** | | | | | | | | | | |
| Percentage of investigations closed or referred for prosecution within 1 year | | 75% | | 93% | | 75% | | | | 75% |
| Number of closed investigations substantiated ** | | ** | | 218 | | ** | | ** | | ** |
| Arrests ** | | ** | | 111 | | ** | | ** | | ** |
| **End Outcome** | | | | | | | | | | |
| Convictions ** | | ** | | 104 | | ** | | ** | | ** |
| Administrative Actions ** | | ** | | 211 | | ** | | ** | | ** |
| Response to Customer Surveys: | | | | | | | | | | |
| Report completed in a timely manner (%) | | 90% | | 100% | | 90% | | | | 90% |
| Issues were sufficiently addressed (%) | | 90% | | 100% | | 90% | | | | 90% |

PERFORMANCE AND RESOURCES TABLE (Goal 1)

**DOJ Strategic Plan:** Supporting the Mission: Efficiency and Integrity in the Department of Justice.

**DIG General Goal #1:** Detect and deter misconduct in programs and operations within or financed by the Department.

**Data Definition, Validation, Verification, and Limitations**

A. **Data Definition:**
The OIG does not project targets and only reports actuals for workload measures, the number of closed investigations substantiated, arrests, convictions, and administrative actions. The number of convictions and administrative actions are not subsets of the number of closed investigations substantiated.

B. **Data Sources, Validation, Verification, and Limitations:**
Investigations Data Management System (IDMS) – consists of a computer-based relational database system that became operational at the end of June 2005. We upgraded the system to a newer release which provides additional functionality. Most of the legacy data from the old IDMS was converted, except for records older than FY 1993, which were archived. We developed new reports to run against the database and verified the accuracy of the conversion. We ran the new reports against historical data and also compared them with historical reports and validated the results. The database administrator runs routine maintenance programs against the database. Database maintenance plans are in place to examine the internal physical structure of the database, backup the database and transaction logs, handle index tuning, manage database alerts, and repair the database if necessary. Currently, the general database backup is scheduled nightly and the transaction log is backed up in 3 hour intervals. We are continuing the process of reducing duplicate person records and incorporating methods to prevent the uploading of additional duplicate person records.

Investigations Division Report of Investigation (ROI) Tracking System - a web-based SQL-Server database was launched in June 2007 to track all aspects of the ROI lifecycle. The ROI and Abbreviated Report of Investigation (AROI) are the culmination of OIG investigations and are submitted to DOJ components. These reports are typically drafted by an agent and go through reviews at the Field Office and at Headquarters levels before final approval by Headquarters. The new ROI Tracking System is integrated with IDMS. By providing up-to-the-minute ROI status information, the Tracking System is expected to be a key tool in improving the timeliness of the Division's reports. The Tracking System also incorporates numerous pre-formatted statistical reports to provide agents and their managers with important performance information.

Investigations Division Monthly Investigative Activity Report – Most of the data for this report was designed into the IDMS application, except for integrity briefing activities and the use of certain investigative techniques. A new tab has been designed to collect the data for this report. Data for integrity briefings can be captured in the time entry notebook.

Investigations Division Administrative Database - an Access database was launched in August, 2005 to track the administration of customer satisfaction questionnaires sent with each completed investigative report to components. The database captures descriptive survey information as well as questionnaire responses. Descriptive information includes the questionnaire form administered, distribution and receipt dates, and component and responding official. The database captures responses to several open-ended questions seeking more information on deficiencies noted by respondents and whether a case was referred for administrative action and its outcome. Questionnaire responses are returned to Investigations Headquarters and are manually entered into the database by Headquarters personnel. No data validation tools, such as double key entry, are used though responses are entered through a front-end Access Form in an effort to ease input and reduce errors.

C. **FY 2009 Performance Report:**
For the workload measure, "Investigations Closed" the OIG has increased focus on more complex and document-intensive cases (e.g., grant and contract fraud) that require more in-depth financial and forensic analysis. The OIG is also diversifying its caseload to extend more investigative coverage to other Department components.

## PERFORMANCE MEASURE TABLE (Goal 1)

**Decision Unit/Program:** OIG/Audits, Inspections, Investigations, and Reviews

**DOJ Strategic Plan:** Supporting the Mission: Efficiency and Integrity in the Department of Justice.

**OIG General Goal #1:** Detect and deter misconduct in programs and operations within or financed by the Department.

| Performance Report | FY 2004 | FY 2005 | FY 2006 | FY 2007 | FY 2008 | FY 2009 | FY 2010 | | FY 2011 |
|---|---|---|---|---|---|---|---|---|---|
| **Workload** | **Actual** | **Actual** | **Actual** | **Actual** | **Actual** | **Actual** | **Target** | **Actuals** | **Target** |
| Number of Cases Opened per 1,000 DOJ employees: | | | | | | | | | |
| Fraud | 0.59 | 0.52 | 0.42 | 0.37 | 0.45 | 0.50 | ** | ** | ** |
| Bribery | 0.75 | 0.58 | 0.61 | 0.71 | 0.36 | 0.30 | ** | ** | ** |
| Rights Violations | 0.19 | 0.31 | 0.27 | 0.13 | 0.16 | 0.15 | ** | ** | ** |
| Sexual Crimes | 0.44 | 0.41 | 0.32 | 0.35 | 0.40 | 0.21 | ** | ** | ** |
| Official Misconduct | 1.06 | 1.03 | 1.27 | 1.53 | 1.27 | 1.28 | ** | ** | ** |
| Theft | N/A | 0.18 | 0.20 | 0.26 | 0.21 | 0.25 | ** | ** | ** |
| **Workload** | | | | | | | | | |
| Investigations closed | 486 | 415 | 441 | 400 | 355 | 367 | 350 | | 352 |
| Integrity Briefings and Presentations to DOJ employees | 183 | 235 | 202 | 296 | 248 | 346 | 150 | | 140 |
| DOJ employees attending Integrity Briefings | 8,287 | 11,239 | 9,308 | 11,269 | 8,342 | 7,545 | 4,200 | | 4,200 |
| **Intermediate Outcome** | | | | | | | | | |
| Percentage of investigations closed or referred for prosecution within 1 year (QSR Measure) | 66% | 66% | 69% | 90% | 78% | 93% | 75% | | 75% |
| Number of closed investigations substantiated (QSR Measure) | 165 | 180 | 239 | 227 | 220 | 218 | ** | ** | ** |
| Arrests | 106 | 69 | 134 | 107 | 115 | 111 | ** | ** | ** |
| **End Outcome** | | | | | | | | | |
| Convictions | 124 | 66 | 112 | 105 | 121 | 104 | ** | ** | ** |
| Administrative Actions | 137 | 154 | 175 | 239 | 231 | 211 | ** | ** | ** |
| Response to Customer Surveys: | | | | | | | | | |
| Report completed in a timely manner (%) | 93% | 94% | 97% | 99% | 98% | 100% | 90% | 90% | 90% |
| Issues were sufficiently addressed (%) | 95% | 91% | 99% | 99% | 99% | 100% | 90% | 90% | 90% |

** Indicators for which the OIG only reports actuals.

## PERFORMANCE AND RESOURCES TABLE (Goal 2)

**Decision Unit:** OIG/Audits, Inspections, Investigations, and Reviews

**DOJ Strategic Plan:** Supporting the Mission: Efficiency and Integrity in the Department of Justice.

**OIG General Goal #2:** Promote the efficiency and effectiveness of Department programs and operations.

| WORKLOAD/RESOURCES | Final Target | | Actual | | Projected | | Changes | | Requested (Total) | |
|---|---|---|---|---|---|---|---|---|---|---|
| | FY 2009 | | FY 2009 | | FY 2010 | | Current Services Adjustment and FY 2011 Program Change | | FY 2011 Request | |
| **Total Costs and FTE** (reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total) | FTE | $000 | FTE | $000 | FTE | $000 | FTE | $000 | FTE | $000 |
| | 453 | $75,681 [$18,967] | 432 | $75,681 [$18,582] | 497 | $84,368 [$19,730] | 13 | $4,424 [$1,338] | 510 | $88,792 [$21,068] |
| **Performance Report and Performance Plan** | | | | | | | | | | |
| **Workload** | | | | | | | | | | |
| Audit and E&I assignments initiated | | 150 | | 159 | | 163 | | 2 | | 165 |
| Percent of Audit CSITAO resources devoted to security reviews of major Dept. information systems | | 86% | | 75% | | 75% | | | | 75% |
| Percent of internal audit assignments that assess component performance measures | | 10% | | 18% | | 18% | | | | 18% |
| Percent of Audit and E&I direct resources devoted to internal reviews of Top Ten Mgt. Challenges and GAO and JMD-identified High-Risk Areas | | 90% | | 94% | | 95% | | | | 95% |
| **Intermediate Outcome** | | | | | | | | | | |
| Audit and E&I assignments completed | | 137 | | 155 | | 164 | | 2 | | 166 |

**PERFORMANCE AND RESOURCES TABLE (Goal 2)**

**Decision Unit:** OIG/Audits, Inspections, Investigations, and Reviews

**DOJ Strategic Plan:** Supporting the Mission: Efficiency and Integrity in the Department of Justice.

**OIG General Goal #2:** Promote the efficiency and effectiveness of Department programs and operations.

| WORKLOAD/RESOURCES | Final Target | | Actual | | Projected | | Changes | | Requested (Total) | |
|---|---|---|---|---|---|---|---|---|---|---|
| | FY 2009 | | FY 2009 | | FY 2010 | | Current Services Adjustment and FY 2011 Program Change | | FY 2011 Request | |
| **Total Costs and FTE** | FTE | $000 | FTE | $000 | FTE | $000 | FTE | $000 | FTE | $000 |
| (reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total) | 453 | $75,681 [$18,697] | 432 | $75,681 [$18,697] | 497 | $84,368 [$19,730] | 13 | $4,424 [$1,349] | 510 | $88,792 [$21,068] |
| **Performance Report and Performance Plan** | | | | | | | | | | |
| **Intermediate Outcome** | | | | | | | | | | |
| Percent of Audit resources devoted to reviews of grants and grant management | | 30% | | 47% | | 45% | | | | 45% |
| Components receiving information system audits | | 5 | | 6 | | 8 | | | | 6 |
| Products issued to the Dept. containing significant findings or information for management decision-making by Audit & E&I | | 109 | | 116 | | 125 | | | | 125 |
| Products issued to Congress by Audit and E&I | | 49 | | 47 | | 67 | | 2 | | 69 |
| Percent of E&I assignments completed within the timeframes established by the IG. | | 70% | | 17% | | 60% | | | | 60% |
| Percent of contract, grant, IGA, and other external audits to be completed in draft within 5 months | | 60% | | 60% | | 64% | | 2% | | 66% |
| Percent of internal audits to be completed within 1 year | | 60% | | 66% | | 70% | | 2% | | 72% |

## PERFORMANCE AND RESOURCES TABLE (Goal 2)

**DOJ Strategic Plan:** Supporting the Mission: Efficiency and Integrity in the Department of Justice.

**OIG General Goal #2:** Promote the efficiency and effectiveness of Department programs and operations.

### Data Definition, Validation, Verification, and Limitations

**A. Data Definition:**

"Assignment" covers all audits (including internals, CFO, and Externals, but **not** Single Act Audits), evaluations, and inspections. "Assignments" may also include activities that do not result in a report or product (e.g., a memorandum to file rather than a report).

**B. Data Sources, Validation, Verification, and Limitations:**

The Audit Division Administrative Management (ADAM) System -- collects information that the regional Audit offices provide to headquarters on the status of assignments and the number of workdays expended monthly. This information is reviewed for accuracy, consolidated, and analyzed to determine trends and provide senior management with information on the status of the Audit Division's workplan and the use of Audit Division resources. ADAM is an integrated database that is regularly adjusted based on management decisions.

Evaluation and Inspections Division Management Tracking System -- tracks all assignments by project number and report number, starting with the initiation date and continuing through the closing date and resolution process and the archiving of work products. The Management Tracking System also includes employee workhours, by job, and semiannual report synopses. The system provides senior management with the data to respond to information requests and to track and report on work activities.

Evaluation and Inspections Division Documentation on file -- consists of hard copies of public and non-publicly disseminated correspondence. Because the material is not captured in E&I's management tracking system, a review and count of the documentation on file is the best way to track these indicators.

**C. FY 2009 Performance Report:** N/A

## PERFORMANCE MEASURE TABLE (Goal 2)

**Decision Unit/Program:** OIG Audits, Inspections, Investigations, and Reviews

**DOJ Strategic Plan:** Supporting the Mission: Efficiency and Integrity in the Department of Justice

**OIG General Goal #2:** Promote the efficiency and effectiveness of Department programs and operations

| Performance Report | FY 2003 | FY 2004 | FY 2005 | FY 2006 | FY 2007 | FY 2008 | FY 2009 | FY 2010 | | FY 2011 |
|---|---|---|---|---|---|---|---|---|---|---|
| **Workload** | Actual | Actual | Actual | Actual | Actual | Actual | Actual | Target | Actuals | Target |
| Audit and E&I assignments initiated | 227 | 140 | 118 | 118 | 134 | 142 | 159 | 153 | | 165 |
| Percent of E&I workdays devoted to follow-up reviews | 19% | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| Percent of Audit CSITAO resources devoted to security reviews of major Dept. information systems | 46% | 51% | 100% | 86% | 66% | 86% | 75% | 75% | | 75% |
| Percent of internal audit assignments that assess component performance measures | 32% | 13% | 10% | 11% | 10% | 10% | 18% | 18% | | 18% |
| Percent of Audit and E&I direct resources devoted to internal reviews of Top Ten Mgt. Challenges and GAO and JMD-identified High-Risk Areas | 55% | 76% | 92% | 85% | 78% | 78% | 94% | 95% | | 95% |
| **Intermediate Outcome** | | | | | | | | | | |
| Audit and E&I Assignments completed | 233 | 123 | 109 | 114 | 133 | 126 | 155 | 154 | | 165 |
| Percent of Audit resources devoted to reviews of grants and grant management | 20% | 38% | 33% | 28% | 25% | 30% | 47% | 45% | | 45% |
| Components receiving information system audits | 7 | 5 | 6 | 4 | 5 | 4 | 6 | 9 | | 6 |
| Products issued to the Dept. containing significant findings or information for mgt decision-making by Audit and E&I | 233 | 124 | 122 | 97 | 102 | 99 | 116 | 125 | | 125 |
| Products issued to Congress by Audit and E&I | 45 | 51 | 51 | 46 | 45 | 48 | 47 | 67 | | 63 |
| Percent of E&I assignments to be completed within 6 months | 50% | 27% | 78% | 64% | 70% | 70% | 17% | 60% | | 60% |
| Percent of contract, grant, IGA, and other external audits to be completed within 5 months | 68% | 71% | 68% | 58% | 60% | 66% | 60% | 64% | | 66% |
| Percent of internal audits to be completed within 1 year | 69% | 43% | 93% | 68% | 60% | 66% | 66% | 70% | | 72% |

## 4. Performance, Resources, and Strategies

a. Performance Plan and Report for Outcomes

For the Department's programs and activities to be effective, Department personnel, contractors, and grantees must conduct themselves in accordance with the highest standards of integrity, accountability, and efficiency. The OIG was established to detect and prevent misconduct and mismanagement on the part of the Department's personnel and in its programs. The OIG investigates alleged violations of criminal and civil laws, regulations, and ethical standards arising from the conduct of the Department's employees in their numerous and diverse activities. In addition, the OIG assists management in promoting integrity, economy, efficiency, and effectiveness within the Department and in its financial, contractual, and grant relationships with others using the coordinated efforts of the OIG's investigative, audit, inspection, and special review resources.

The OIG continues to review its performance measures and targets, especially in light of the changing nature of the cases it investigates and the nature of the Department programs it reviews. Today's work is much more complex and expansive than it was only a few years ago. The number of documents to be reviewed, the number of people to interview, the amount of data to examine, and the analytical work involved in many OIG reviews are significantly greater than in prior years. This is especially true for reviews of sensitive Department programs such as the review of the Department's role in the President's Surveillance Program, as well as cross-cutting work that covers multiple components, such as the OIG's reviews of components use of less than lethal weapons, disciplinary programs, or litigation case management systems. These multi-component reviews can be particularly valuable in identifying "best practices" within the Department and ensuring consistency across component programs.

b. Strategies to Accomplish Outcomes

The OIG will investigate allegations of bribery, fraud, abuse, civil rights violations, and violations of other laws and procedures that govern Department employees, contractors, and grantees, and will develop cases for criminal prosecution and civil and administrative action. The OIG will use its audit, inspection, and attorney resources to review Department programs or activities identified as high-priority areas in the Department's strategic plan and devote resources to review the Department's Top Management and Performance Challenges.

**VI. Program Increases by Item**
**Item Name: Enhanced Oversight of DOJ's National Security Programs**

| | |
|---|---|
| Budget Decision Unit: | Audits, Inspections, Investigations, and Reviews |
| Strategic Goal & Objective: | Supporting the Mission: Efficiency and Integrity in the Department of Justice |
| Organizational Program: | OIG |

Program Increase: Positions **+8** Agt/Atty **+0/+0** FTE **+4** Dollars **+$609,000**

Description of Item
The OIG is requesting 4 program analysts and 4 auditors for Enhanced Oversight of the Department's national security programs.

**Justification**
The requested positions would be deployed to enhance the OIG's oversight of national security programs and further support the OIG's ability to meet its increased demands to adequately and effectively monitor the Department's counterterrorism resources, cybercrime activities, and its efforts to improve sharing of intelligence and law enforcement information.

These new resources would allow the OIG to undertake several new assignments in critical areas. For example, the increased resources would further assist our efforts to effectively conduct future USA Patriot Act reviews. The *USA Patriot Improvement and Reauthorization Act of 2005* (Reauthorization Act), Public Law No. 109-177, required the Department of Justice's OIG to conduct reviews of the FBI's use of certain authorities established or expanded by the USA Patriot Act, Public Law No. 107-56, as amended. With these additional resources, the OIG will continue to examine critical issues such as the use and effectiveness of the FBI's authority to issue national security letters and 215 orders to obtain business records, as well as their use of FISA pen register and trap and trace devices during the calendar years 2007, 2008, and 2009.

In addition, we plan to conduct reviews related to the Foreign Surveillance Intelligence Act (FISA) U.S. Persons Collections Program. Section 702 of the FISA Amendments Act of 2008 established procedures for conducting electronic surveillance on certain persons outside the United States other than U.S. persons. It also directed the DOJ OIG to conduct a review of: the number of disseminated intelligence reports containing a reference to a U.S. person identity; the number of U.S. person identities subsequently disseminated in response to requests for identities not referred to by name or title in the original reporting; and the number of targets later determined to be located in the U.S., and to the extent possible, whether communications of such targets were reviewed. The legislation also authorizes the OIG to review compliance with targeting and minimization procedures that were adopted to conduct the program described in Section 702.

These increased resources will also support the OIG's ongoing and planned audits of the Department's efforts to combat cybercrime. Cybercrime already poses a significant and growing threat to U.S. national economic interests, but as computers and other information technology systems have become part of our critical infrastructure, protection of these systems is central to our national security. The OIG is conducting an audit that is evaluating the FBI's efforts to

develop and operate the National Cyber Investigative Task Force (NCIJTF) to address potential national security cyber threats. The audit also is examining the FBI field offices' capabilities to investigate national security cyber cases.

Additional resources would also support other ongoing and planned audits and reviews on national security topics such as the Department's efforts to address terrorists financing and its preparations for responding to a weapons of mass destruction attack. The OIG also plans to undertake a review assessing the effectiveness of the FBI's Office of Integrity and Compliance, which is responsible for monitoring the FBI's compliance with laws, regulations, and FBI policies.

In sum, DOJ must continue to respond to the growing challenge to its national security programs. Providing additional resources to the OIG will further enhance our ability to help the Department meet this challenge.

## Funding

(Dollars in Thousands)

The OIG operates as a single decision unit encompassing audits, inspections, investigations, and reviews. By the nature of its mission, the OIG must be able to move its resources and funding freely across all functions to address new priorities. Therefore, base funding for the OIG is only meaningful at the single decision unit level.

Personnel Increase Cost Summary

| Type of Position | Modular Cost Per Position ($000) | Number of Positions Requested | FY 2011 Request ($000) | FY 2012 Net Annualization ($000) |
|---|---|---|---|---|
| Program Analyst (GS-11) | $76 | 4 | $305 | $198 |
| Auditor (GS-11) | $76 | 4 | $305 | $198 |
| **Total Personnel** | | **8** | **$609** | **$396** |

Total Request for This Item

| | Pos | Agt/Atty | FTE | Personnel | Non-Personnel | Total |
|---|---|---|---|---|---|---|
| Increases | 8 | 0/0 | 4 | $609 | $0 | $609 |
| **Grand Total** | **8** | **0/0** | **4** | **$609** | **$0** | **$609** |

**Item Name: Funding for Council of the Inspectors General on Integrity and Efficiency (CIGIE) Operations**

Budget Decision Unit: Audits, Inspections, Investigations, and Reviews
Strategic Goal & Objective: Supporting the Mission: Efficiency and Integrity in the Department of Justice
Organizational Program: OIG

Program Increase: Positions **+0** Agt/Atty **+0/+0** FTE **+0** Dollars **+$394,000**

Description of Item
The OIG is requesting $394,000 to fund its support of the governmentwide efforts of the Council of the Inspectors General on Integrity and Efficiency (CIGIE).

Justification
In previous fiscal years, the OIG's contribution to funding CIGIE activities has come directly out of its base resources, thus reducing its operations funding for audits, investigations, inspections, and reviews. With this much-needed program increase, the OIG can restore this base funding and focus these direct resources to initiate further actions that save taxpayers' dollars and cut waste.

**Funding**
(Dollars in Thousands)

The OIG operates as a single decision unit encompassing audits, inspections, investigations, and reviews. By the nature of its mission, the OIG must be able to move its resources and funding freely across all functions to address new priorities. Therefore, base funding for the OIG is only meaningful at the single decision unit level.

Total Request for This Item

| | Pos | Agt/Atty | FTE | Personnel | Non-Personnel | Total |
|---|---|---|---|---|---|---|
| Increases | 0 | 0/0 | 0 | $0 | $394 | $394 |
| **Grand Total** | **0** | **0/0** | **0** | **$0** | **$394** | **$394** |

**VI. Program Decreases by Item**
**Item Name: Travel Management and Efficiencies**

| | |
|---|---|
| Budget Decision Unit: | Audits, Inspections, Investigations, and Reviews |
| Strategic Goal & Objective: | Supporting the Mission: Efficiency and Integrity in the Department of Justice |
| Organizational Program: | OIG |

Program Decrease: Positions **-0** Agt/Atty **-0/-0** FTE **-0** Dollars **($173,000)**

Description of Item
The Department is continually evaluating its programs and operations with the goal of achieving across-the-board economies of scale that result in increased efficiencies and cost savings. In FY 2011, DOJ is focusing on travel as an area in which savings can be achieved. For the OIG, travel or other management efficiencies will result in offsets of $173,000. This offset will be applied in a manner that will allow the continuation of effective law enforcement program efforts in support of Presidential and Departmental goals, while minimizing the risk to health, welfare, and safety of agency personnel.

**Funding**
(Dollars in Thousands)

The OIG operates as a single decision unit encompassing audits, inspections, investigations, and reviews. By the nature of its mission, the OIG must be able to move its resources and funding freely across all functions to address new priorities. Therefore, base funding for the OIG is only meaningful at the single decision unit level.

Total Offset for This Item

| | Pos | Agt/Atty | FTE | Personnel | Non-Personnel | Total |
|---|---|---|---|---|---|---|
| Decreases | 0 | 0/0 | 0 | $0 | -$173 | -$173 |
| **Grand Total** | **0** | **0/0** | **0** | **$0** | **-$173** | **-$173** |