

Department of Justice
Office of the Inspector General
Estimates for FY 2008 Congressional Budget
Table of Contents

	<u>Page No.</u>
I. Overview	1
II. Summary of Program Changes	3
III. Appropriations Language and Analysis of Appropriations Language	4
IV. Decision Unit Justification	5
A. OIG	5
Program Description	5
Performance Measurements	6
Performance and Resources Table	20
Performance, Resources, and Strategies	28
Program Increases	28
V. Exhibits	
A. Organization Chart	31
B. Summary of Requirements	32
C. Program Increases/Offsets by Decision Unit	34
D. Resources by DOJ Strategic Goal and Strategic Objective	35
E. Justification for Base Adjustments	36
F. Crosswalk of 2006 Availability	38
G. Crosswalk of 2007 Availability	39
H. Summary of Reimbursable Resources	40
I. Detail of Permanent Positions by Category	41
J. Financial Analysis of Program Changes	42
K. Summary of Requirements by Grade	43
L. Summary of Requirements by Object Class	44
M. Status of Congressionally Requested Studies, Reports, and Evaluations	45

I. Overview for Office of the Inspector General FY 2008 Congressional Budget Request

1. Introduction

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 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); 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 effectiveness.

In fiscal year (FY) 2008, the Department's top priority will continue to be detecting and preventing terrorism. The Department requested more than \$3.4 billion towards that effort in FY 2007. The Department also estimates that it will request \$2.2 billion for information technology (IT) annually. The OIG, through its audits, inspections, investigations, and reviews, will help ensure that the substantial funding provided to support these Attorney General priorities 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, strengthening the Department's internal financial systems, improving grant management and accountability, ensuring the effectiveness and security of computer systems, and promoting public confidence in the integrity of the Department's programs and employees. The OIG's request for FY 2008 totals \$73,208,000, 439 full-time permanent positions, and 425 direct workyears. This request represents an adjustment-to-base increase of \$2,896,000, and program enhancements for 5 positions, 3 workyears and \$460,000 for Counterterrorism Oversight.

The OIG helps the Department pursue its strategic goals and objectives through its investigations, audits, inspections, and program reviews. The OIG has two general goals that support the Department's strategic goals: To "detect and deter misconduct in programs and operations within or financed by the Department," and to "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 targets resources on reviews of Department programs to promote the economy, efficiency, and effectiveness of those programs.

To be successful, the OIG must deal with a variety of internal and external challenges that affect its work. These include the decisions Department employees make while carrying out their numerous and diverse duties that may increase or decrease the number of allegations the OIG receives; Department support for the OIG's fulfillment of its duties and responsibilities; and financial support from the Office of Management and Budget and Congress.

The OIG's biggest internal challenge is in the area of human capital. The OIG is working to ensure that it continues to hire employees who have the appropriate skill sets for its complex mission.

Finally, the OIG has not been selected for a Program Assessment Rating Tool (PART) review.

Note: Beginning in FY 2007, 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/2008justification/>.

II. Summary of Program Changes

Office of the Inspector General (\$ in thousands)					
Item Name	Description	Pos.	FTE	Dollars	Page
Counterterrorism Oversight	The OIG is requesting 3 auditors, 1 program analyst and 1 attorney for Counterterrorism Oversight.	5	3	\$460	28
	Total	5	3	\$460	

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 Inspector General, \$73,208,000, including not to exceed \$10,000 to meet unforeseen emergencies of a confidential character.

Analysis of Appropriations Language

No substantive changes proposed.

Note: The FY 2008 President's Budget uses the FY 2007 President's Budget language as a base so all language is presented as new.

IV. Decision Unit Justification

A. OIG

The OIG is one decision unit.

OIG	Perm. Pos.	FTE	Amount
2006 Enacted w/Rescissions and Supplementals	449	449	67,922,000
2007 Estimate	449	459	69,852,000
Adjustments to Base and Technical Adjustments	-15	-14	2,896,000
2008 Current Services	434	445	72,748,000
2008 Program Increases	5	3	460,000
2008 Offsets
2008 Request	439	448	73,208,000
Total Change 2007-2008	5	3	3,356,000

Note: The FTEs above include reimbursables.

1. Program Description

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

PERFORMANCE MEASUREMENTS

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

The OIG does not set targets for certain law enforcement activities since those measures could be construed as “bounty hunting.” For such law enforcement measures, the OIG reports historical results.

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

The FBI’s Sentinel Case Management System

Since 2002, the OIG has reviewed and monitored the FBI’s efforts to upgrade its IT systems. The most recent effort is the FBI’s Sentinel program, a project to replace the FBI’s antiquated Automated Case Support system with a modern case management system.

In March 2006, the OIG released the first in a series of audits that will monitor the FBI’s development and implementation of the Sentinel project. Sentinel is the successor to the \$170 million Virtual Case File (VCF) project that the FBI ended unsuccessfully after 3 years. Reviews by the OIG found that the VCF project failed for a variety of reasons, including poorly defined and slowly evolving design requirements, weak IT investment management practices, weaknesses in the way contractors were retained and overseen, the lack of management continuity at the FBI on IT projects, unrealistic scheduling of tasks, and inadequate resolution of issues that warned of problems in project development.

In light of these issues, the OIG’s March 2006 audit evaluated the FBI’s progress on the Sentinel project. We assessed the FBI’s pre-acquisition planning for Sentinel, including the approach, design, cost, funding sources, time frame, contracting vehicle, and oversight structure. The OIG found that the FBI has taken important steps to help prevent the types of problems encountered in the VCF project. In reviewing the management processes and controls the FBI has applied to the pre-acquisition phase of Sentinel, the OIG found that the FBI has developed IT planning processes that, if implemented as designed, can help the FBI successfully complete Sentinel.

In particular, the OIG found that the FBI has made improvements in its ability to plan and manage a major IT project by establishing IT Investment Management processes, developing a more mature Enterprise Architecture, and establishing a Program Management Office (PMO) dedicated to the Sentinel project.

However, the OIG identified several continuing concerns about the FBI’s management of the Sentinel project: (1) the incomplete staffing of the Sentinel Program Management Office, (2) the FBI’s ability to reprogram funds to complete the second phase of the project without jeopardizing its mission-critical operations, (3) Sentinel’s ability to share information with

external intelligence and law enforcement agencies and provide a common framework for other agencies' case management systems, (4) the lack of an established Earned Value Management process, (5) the FBI's ability to track and control Sentinel's costs, and (6) the lack of complete documentation required by the FBI's IT Investment Management processes.

In addition, while the FBI has considered its internal needs in developing Sentinel's requirements, the OIG review expressed concern that the FBI had not yet adequately examined or discussed Sentinel's ability to connect with external systems in other Department components, the Department of Homeland Security (DHS), and other intelligence community agencies. If such connectivity is not built into Sentinel's design, other agencies could be forced into costly and time-consuming modifications to their systems to allow information sharing with the Sentinel system.

In December 2006, we issued the second Sentinel audit and found that the FBI has made significant progress in addressing many of the concerns highlighted in our first audit. However, some concerns still remain, and we also identified several additional issues, such as an uncertainty over total project costs and a lack of contingency planning for identified project risks that warrant continued monitoring by the FBI. This report contains 5 recommendations that focus on further reducing risks to the Sentinel project, including updating the estimate of total project costs as actual cost data becomes available, developing contingency plans for significant project risks, and filling vacancies in the Sentinel PMO. The FBI concurred with all our recommendations.

In early 2007, the OIG will open its third review of the Sentinel project.

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

In March 2006, the OIG released an audit report that examined the FBI's efforts to protect U.S. seaports from terrorism. The United States has more than 360 seaports, and 95 percent of overseas trade flows through these ports or inland waterways, which often are located near major population centers. The protection of U.S. seaports is a shared responsibility among the DHS, U.S. Coast Guard, U.S. Customs and Border Protection, and FBI. The Coast Guard protects and enforces laws at seaports while the Customs and Border Protection enforces import and export laws and inspects cargo at seaports. The FBI, as the lead federal agency for preventing and investigating terrorism, has an overarching role in protecting the nation's seaports, which includes gathering intelligence on maritime threats and maintaining well-prepared tactical capabilities to prevent or respond to maritime-based terrorism. Because of the number of different agencies involved with the nation's seaport security efforts, the issue of efficient and effective information sharing takes on vital importance.

The OIG review of the FBI's efforts to protect the nation's seaports found that since the September 11 attacks, the FBI has taken steps to enhance its capability to identify, prevent, and respond to terrorist attacks at seaports. For example, the FBI has created a centralized maritime security program at FBI Headquarters and, in addition to its counterterrorist tactical teams, has placed enhanced maritime SWAT teams in the FBI field offices closest to 14 of the nation's strategic seaports. Further, most of the FBI's 56 field offices have Maritime Liaison Agents responsible for coordinating with other federal agencies on maritime security.

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

Furthermore, the OIG review found that the FBI and the Coast Guard have not yet resolved issues regarding their overlapping responsibilities, jurisdictions, and capabilities to handle a maritime terrorism incident. We believe a lack of jurisdictional clarity could hinder the FBI's and the Coast Guard's ability to coordinate an effective response to a terrorist threat or incident in the maritime domain. Specifically, the report expressed concern about how confusion over authorities will affect the two agencies' ability to establish a clear and effective incident command structure in response to a terrorist attack on a seaport. In our judgment, unless such differences over roles and authorities are resolved, the response to a maritime incident could be confused and potentially disastrous.

The OIG report made 18 recommendations that focus on specific steps that the FBI should take to improve its counterterrorism efforts regarding seaport and maritime activities, including resolving overlapping responsibilities with the Coast Guard before a terrorist incident occurs; leading more interagency maritime-related exercises involving likely terrorism scenarios; preparing and using after-action reports after these exercises in order to identify lessons learned; and assessing the threat and risk of maritime terrorism compared to other threats and assigning resources accordingly.

Review of the Terrorist Screening Center

In December 2003, the Terrorism Screening Center (TSC) began operating as the nation's single point of contact for law enforcement authorities requesting assistance in the identification of individuals with possible ties to terrorism. The OIG's June 2005 audit report on TSC operations found that TSC management successfully created a new organization and consolidated vast amounts and types of terrorist information, which are significant accomplishments. However, our review found several areas of TSC operations needing improvement. The creation of the consolidated database, a phased approach that continues to evolve, has weaknesses that need to be addressed. Database controls and improved search capabilities are necessary to ensure that watchlist data is safeguarded, database history is retained, and call screeners are able to readily identify individuals encountered. Procedures for verifying the completeness and accuracy of records within the TSC database also need to be enhanced to ensure that records are included in a timely manner, all record information consolidated into the database is complete and accurate, and measures taken to ensure any missing, conflicting, or duplicate information is identified and resolved on a regular basis. Further, a lack of sufficient training, oversight, and general management of the call screeners has left the activities of the call center vulnerable to procedural errors, poor data entry, and untimely responses to callers.

The OIG report provided 40 recommendations to the TSC to address areas such as database improvements, data accuracy and completeness, call center management, operational planning, coordination between participating agencies, and staffing. The TSC generally agreed with the recommendations and said it was in the process of taking corrective action.

In late 2006, we initiated a follow-up audit of the TSC. Our objectives are to determine if accurate and complete records are disseminated to and from the watchlist database in a timely fashion; review the TSC's efforts to ensure the quality of the information in the watchlist database; and assess the TSC's ability to correct records where individuals are incorrectly identified as watchlist subjects.

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

In September 2006, the OIG issued a report that evaluated the BOP's efforts to prevent terrorists and other high-risk inmates from using the mail or the cover of a foreign language to commit criminal or terrorist activities. The OIG review concluded that the BOP's monitoring of inmate mail and other forms of communication was deficient in several respects: 1) the BOP does not read all the mail for terrorists and other high-risk inmates on its mail monitoring lists, 2) the BOP does not have enough proficient translators to translate inmate mail written in foreign languages, and 3) the BOP does not have sufficient staff trained in intelligence techniques to analyze whether terrorists' communications contain suspicious content. In addition to the deficiencies in its mail monitoring efforts, the OIG also found that the BOP is unable to effectively monitor high-risk inmates' verbal communications, which include telephone calls, visits with family and friends, and cellblock conversations.

According to BOP officials, BOP staff is expected to read 100 percent of the mail for inmates placed on mail monitoring lists. However, staff members at 7 of the 10 institutions that we visited told us they were not reading 100 percent of the mail for these inmates, and the percentage of mail read had decreased since FY 2005 due to staff reallocations.

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

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

In general, we found that the BOP's intelligence capability to analyze the contents of terrorist inmates' mail is not well developed. The BOP offers only limited intelligence training to its staff to enable them to identify suspicious content in the mail of terrorist inmates. The OIG also found that the BOP was not meeting its own internal goals for telephone monitoring of high-risk inmates, and thus, may be missing opportunities to gather intelligence about terrorist or criminal activity. In addition, we found that the Department does not have a policy requiring that all inmates arrested for international terrorism-related crimes be reviewed to determine whether they should be placed under Special Administrative Measures (SAMs), the most restrictive conditions that can be placed on an inmate's communications. We concluded that unless such a review is

required, there is no guarantee that international terrorist inmates will receive the heightened security and communications monitoring they require during incarceration.

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

The OIG made 13 recommendations designed to strengthen these initiatives and provide additional improvements to the BOP's monitoring of mail and verbal communications of terrorists and high-risk inmates. Two additional recommendations were addressed to the FBI and the Criminal Division. The BOP, Criminal Division, and FBI concurred with all 15 recommendations and have begun to develop plans to implement these recommendations.

September 2005 Shooting Incident Involving the FBI and Ojeda Rios

In August 2006, the OIG issued a report examining the September 2005 shooting incident involving the FBI and long-time fugitive Filiberto Ojeda Rios, leader of a Puerto Rican pro-independence organization that claimed credit for various violent crimes during the late 1970s and 1980s. Journalists, elected officials, and activists in Puerto Rico criticized the FBI for using excessive force to capture Ojeda and for waiting 18 hours after Ojeda was shot before entering his residence, thereby allowing Ojeda to bleed to death. The FBI Director requested that the OIG conduct an investigation to determine the facts and circumstances of the Ojeda shooting incident and to make recommendations regarding what actions, if any, the FBI should take in connection with it.

The OIG's objective in conducting this review was to investigate the facts relating to the incident: (1) to determine whether the FBI agents involved in the operation complied with the Department's Deadly Force Policy, (2) to assess the FBI's decision to conduct an emergency daylight assault of the Ojeda residence in light of other potential options for apprehending Ojeda, (3) to assess the FBI's planning for and conduct of negotiations with Ojeda during a standoff following an initial exchange of gunfire, (4) to determine the reasons the FBI waited 18 hours after the shooting to enter the residence, and (5) to evaluate communications between the FBI, the Commonwealth of Puerto Rico, and the public regarding the operation.

The OIG investigation was conducted by a team of OIG attorneys and special agents. In the course of the investigation, the OIG interviewed over 60 individuals, including the FBI agents involved in the attempted arrest of Ojeda, FBI Headquarters officials, officials from the USAO's Office in Puerto Rico, and officials from the Department of Justice of the Commonwealth of Puerto Rico and the Police of Puerto Rico. The OIG also conducted lengthy interviews of the Executive Director of the Puerto Rico Institute of Forensic Sciences, and other scientists involved in preparing the forensic reports. In addition, the OIG reviewed thousands of

pages of documents generated by the FBI and the USAO relating to the Ojeda matter, and relevant forensic reports prepared by the Puerto Rico Institute of Forensic Sciences, including the autopsy report, bullet and shell casing analyses, trajectory analysis, shooting reconstruction, and blood pattern analysis. Finally, the OIG consulted with three outside experts in tactical police operations to provide expert input and guidance on the FBI's tactical decisions in the Ojeda operation and application of the Department's Deadly Force Policy.

The OIG investigation found that Ojeda opened fire on the federal agents as they attempted to enter his residence in Puerto Rico. Three FBI agents were shot and one was seriously wounded. The OIG concluded that once Ojeda began firing he posed an imminent danger of death or serious injury to the agents and that under the Department's Deadly Force Policy the agents were justified in returning fire at Ojeda. The report also examined the reasons that the agents did not enter the residence until more than 18 hours after Ojeda was shot. The OIG concluded that the FBI's cautious approach toward entering the residence after Ojeda was shot was motivated by consideration of agent safety, not by any desire to withhold medical treatment from Ojeda or to let him die.

However, the OIG report cited deficiencies in several aspects of the planning and execution of the attempted arrest. For example, the investigation determined that the decision to conduct an emergency daylight assault to arrest Ojeda on September 23 was extremely dangerous and was not the best option available. The OIG concluded that a strategy of surrounding the residence and calling for Ojeda to surrender, with the option of using chemical agents such as tear gas to force Ojeda outside, would have been a safer and more effective strategy. The report made 10 systemic recommendations intended to improve the planning and conduct of future FBI arrest operations, including assuring the reconsideration of all relevant tactical options when circumstances change and ensuring that negotiations are integrated into tactical planning for operations in which a standoff is a foreseeable contingency.

The FBI's Handling of the Brandon Mayfield Matter

In January 2006, the OIG issued a report on the FBI's conduct in connection with the identification of a fingerprint found on evidence from the March 2004 terrorism attack on commuter trains in Madrid, Spain, that killed almost 200 people and injured more than 1,400. FBI fingerprint examiners erroneously concluded that the fingerprint found on a bag of detonators belonged to Brandon Mayfield, an attorney in Portland, Oregon. As a result of the misidentification, the FBI initiated an investigation of Mayfield that resulted in his arrest as a material witness. Mayfield was released 2 weeks later when the Spanish National Police identified an Algerian national as the source of the fingerprint on the bag. The FBI Laboratory subsequently withdrew its fingerprint identification of Mayfield.

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

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

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

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

The OIG did not find evidence that the FBI misused any of the provisions of the *USA PATRIOT Act* (Patriot Act) in conducting its investigation of Mayfield. However, the increased information sharing permitted by the Patriot Act amplified the consequences of the FBI's fingerprint misidentification.

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

The FBI's Oversight of Counterintelligence Asset Katrina Leung

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

The OIG investigation was conducted by a team of OIG attorneys and agents. In the course of the investigation, the OIG conducted over 120 interviews and reviewed more than 330,000 pages of documents. The OIG report found that Smith operated Leung with little oversight based primarily on his status as a top agent in Los Angeles and Leung's status as a highly valued asset. The OIG determined that the FBI was aware of serious counterintelligence concerns about Leung

that began to surface during the late 1980s and early 1990s but did little to follow up on the warning signals it received.

The OIG report concluded that the FBI's inattention to the oversight of Smith and Leung, its willingness to exempt Smith from complying with the rules governing asset handling, and its failure to aggressively question Smith or follow up when red flags arose allowed Leung to deceive the FBI about the extent of her spying for the People's Republic of China and permitted Smith to continue his affair with Leung until his retirement in November 2000.

In May 2000, the FBI received credible information indicating that Leung was a spy for the People's Republic of China and that she had a source in the FBI's Los Angeles Division office. Yet, the FBI inappropriately informed Smith about this information (which implicated him), and did not begin an investigation of Smith and Leung until May 2001. The OIG concluded that in light of the serious nature and specificity of the allegation, there was no reasonable explanation for the FBI's year-long delay in opening the investigation.

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

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

In June 2006, the OIG released an unclassified version of the full report it completed in 2004 entitled, "A Review of the FBI's Handling of Intelligence Information Prior to the September 11 Attacks." The OIG provided the full report in 2004 to the FBI, Department, Congress, Central Intelligence Agency, National Security Agency, and National Commission on Terrorist Attacks Upon the United States. The OIG's 2004 report is classified at the Top Secret/Sensitive Compartmented Information level.

At the request of members of Congress, the OIG also created an unclassified version of the report for public release. However, because the unclassified version included information about the FBI's investigation of Zacarias Moussaoui, and because Moussaoui's trial was pending at the time, the OIG could not release the portions of the unclassified report relating to Moussaoui. The OIG therefore publicly released the unclassified report in June 2005 without any of the information relating to Moussaoui.

The Moussaoui case concluded in May 2006 when the U. S. Court for the Eastern District of Virginia sentenced Moussaoui to life in prison. On June 19, 2006, the OIG released an unclassified version of the full report that includes both the Moussaoui chapter and the other references to Moussaoui throughout the report that previously had not been released publicly.

The OIG report found significant deficiencies in the FBI's intelligence information related to September 11 and concluded that the FBI failed to fully evaluate, investigate, exploit, and disseminate the information it had received about efforts by Usama Bin Laden to send students to attend United States civil aviation schools to conduct terrorist activities and intelligence information regarding two of the September 11 hijackers. In the final report, the OIG made 16 recommendations for improving the FBI's intelligence and counterterrorism efforts, including recommendations targeted towards the FBI's analytical program.

FBI's Foreign Language Translation Program

In July 2005, the OIG issued a follow-up audit of the FBI's Foreign Language Translation Program. The follow-up review assessed the FBI's progress in responding to recommendations contained in the OIG's July 2004 audit of the foreign language program and in addressing the volume of unreviewed counterterrorism and counterintelligence audio material (backlog) that it collects from its National Foreign Intelligence Program. The follow-up review concluded that the FBI has taken important steps to address the OIG's recommendations and has made progress to improve the operations of the Foreign Language Program, but key deficiencies remained.

For example, the FBI now sets specific target staffing levels for linguists that account for attrition and, as of March 30, 2005, had achieved 56 percent of current hiring goals. In addition, the FBI has begun to identify counterterrorism cases with significant backlogs and has addressed issues with storage limitations on its digital collection system that can result in the deletion of unreviewed audio sessions. Although the OIG found that the FBI continued to delete unreviewed translation materials, no unreviewed counterterrorism or Al Qaeda sessions had been deleted.

However, the OIG found that key deficiencies remain in the FBI's Foreign Language Translation Program. These deficiencies include a continuing backlog of unreviewed material, some instances where high-priority material has not been reviewed within 24 hours in accord with FBI policy, and continued challenges in meeting linguist hiring goals and target staffing levels. In addition, implementation of the Quality Control Program has been slow, although the FBI has made recent improvements in this area.

The follow-up review found that the FBI's collection of audio material continues to outpace its ability to review and translate that material, with the amount of unreviewed FBI counterterrorism and counterintelligence audio material increasing since our July 2004 report. While the FBI believes that most of the unreviewed material may not need to be translated, it has no assurance that all such counterterrorism and counterintelligence material should not be reviewed or translated.

Possible Intelligence Violations Reported to the Intelligence Oversight Board

Section 1001 of the Patriot Act directs the OIG to undertake a series of actions related to claims of civil rights or civil liberties violations allegedly committed by Department employees. In March 2006, the OIG released its eighth semiannual report to Congress required by Section 1001. The report described the OIG's activities during the last 6 months related to civil rights and civil liberties complaints and the status of OIG and Department investigations of allegations of civil rights and civil liberties abuses by Department employees.

In addition to summarizing investigations and reviews undertaken by the OIG in furtherance of our Section 1001 responsibilities, the March Section 1001 report described the results of an OIG review of the FBI's reporting to the President's Intelligence Oversight Board (IOB) of possible intelligence violations. Our report detailed the types and percentages of violations reported by the FBI to the IOB in FYs 2004 and 2005 and the process used by the FBI to report such violations. Under the FBI's process, FBI employees self-report potential violations to the FBI's Office of the General Counsel, which reviews the possible violations to determine whether reporting to the IOB is required. Among the authorities the FBI used during this period that prompted reports to the IOB were the Foreign Intelligence Surveillance Act of 1978 (FISA), including FISA authorities that were expanded by the Patriot Act; the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection; and various statutory authorities used to issue National Security Letters to obtain information from third parties.

Examples of the violations that the FBI reported to the IOB in FYs 2004 and 2005 include FBI agents intercepting communications outside the scope of the order from the FISA Court; FBI agents continuing investigative activities after the authority for the specific activity expired; and third parties providing information that was not requested by the National Security Letter. Not all possible violations were attributable solely to FBI conduct. According to the data we reviewed, third parties such as telephone companies were involved in or responsible for the possible violations in approximately one-quarter of the cases in both years we examined. The OIG's Section 1001 report also provided detailed information that summarized the percentages of possible violations reported to the IOB, broken down by specific intelligence activity. We intend to report on potential IOB violations in early 2007.

Review of ATF's Violent Crime Impact Team Initiative

In May 2006, the OIG issued a review of ATF's Violent Crime Impact Team (VCIT) initiative that seeks to decrease homicides and violent crimes committed with firearms in targeted urban areas. VCITs currently operate in 23 cities across the country, and the initiative is slated to expand by 15 additional cities by FY 2008. The VCIT strategy includes targeting specific geographic areas or "hot spots" with a high rate of firearms violence, targeting the "worst-of-the-worst" violent offenders in those areas, building effective working relationships with community leaders, using ATF firearms investigative technology resources, and involving representatives from other Department law enforcement components.

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

We also concluded that ATF could not support its claim in its January 2006 report on best practices that the number of homicides committed with firearms was lower in 13 of the 15 VCIT pilot cities' target areas compared to the same 6-month period the preceding year.

The OIG made 5 recommendations to improve ATF's implementation of the VCIT initiative, including establishing specific operational guidelines for VCIT implementation and developing an adequate evaluation strategy to assess the success of the VCIT program. ATF, while disagreeing with some of the findings in the OIG report, concurred with all our recommendations and is implementing the recommendations.

DEA Drug Diversion Control Program

In July 2006, the OIG issued a follow-up report that addressed the DEA's actions to control pharmaceutical diversion since our previous review in October 2002. We found that the DEA has taken important steps to improve its ability to control the diversion of controlled pharmaceuticals, especially pharmaceutical diversion using the Internet. However, several shortcomings that we identified and reported on in 2002 still exist.

On the positive side, in our current review, the OIG found that the DEA has made diversion control a strategic goal, established performance measures for diversion control, centralized its diversion criminal investigations with other criminal investigations, and provided additional intelligence resources to diversion investigators. The DEA also increased the number of authorized domestic diversion investigator positions by 75, from 512 in FY 2004 to 587 in FY 2005. The number of criminal diversion investigations the DEA initiated rose from 770 in FY 2002 to 950 in FY 2005 – an increase of 23 percent.

Moreover, since 2002 the DEA has taken a series of actions to control the increasing use of the Internet to divert pharmaceuticals. From FY 2002 to FY 2005, it increased the percentage of time that diversion investigators spent investigating Internet diversion cases from 3 percent to 11 percent. The DEA also developed an operational strategy for Internet diversion investigations. Among the elements of the strategy that we examined we found that the Online Investigations Project, under development since 2001, has become a valuable investigative tool even though it cannot automatically identify websites with the highest volume of suspect pharmaceutical sales as originally intended.

Despite these positive actions, we identified several continuing concerns. Although the need for special agent assistance in diversion investigations had increased significantly since our previous review, we found that the time spent by special agents assisting diversion investigations still constitutes a small share of their total investigative effort. While the DEA still has not resolved the complicated issue of providing law enforcement authority for its diversion investigators so that diversion investigators are able to perform the law enforcement tasks that are critical to completing criminal investigations, it is actively pursuing the matter. Further, the support intelligence analysts provide to diversion groups in the field has continued to be limited, and intelligence analysts and special agents still receive minimal diversion control training.

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

The Department's Terrorism Task Forces

In June 2005, the OIG reviewed the Department's terrorism task forces, including the Deputy Attorney General's National Security Coordination Council; the U.S. Attorneys' Anti-Terrorism Advisory Councils; and the FBI's Joint Terrorism Task Forces (JTTF), the National Joint Terrorism Task Force and the Foreign Terrorist Tracking Task Force. These task forces and councils are responsible for coordinating and integrating intelligence and law enforcement functions to eliminate terrorist networks, preventing terrorist operations, and prosecuting perpetrators of terrorist acts. The OIG examined whether these terrorism task forces and councils were achieving their purposes; whether gaps, duplication, and overlap existed in counterterrorism coverage; and how the performance of the task forces and councils was measured.

The OIG found that the task forces and councils were achieving their intended purpose. They provided distinct, yet complementary, forums for investigating terrorist threats and for sharing counterterrorism information, particularly among federal, state, and local law enforcement agencies. However, the OIG review found key areas that needed improvement. The review identified several management and resource problems, including the need for more stable leadership among the task forces and councils, more explicit direction, adequate resources, better training for participants, and better coverage of remote areas.

In addition, in some instances the groups were understaffed or lacked personnel with particular types of expertise because certain agencies had chosen to limit their participation or had provided staff without the appropriate expertise. The OIG also found that for the JTTFs, no national training plans or minimum training standards had been developed, participants were notified of training opportunities on an ad hoc basis, and many participants believed that FBI participants received preferential treatment.

The OIG's report contained 28 recommendations to help the Department improve the operations of the counterterrorism task forces and councils, including to stabilize leadership of the groups; establish performance measures and outcome-oriented goals; clarify responsibilities and priorities; develop and implement national training plans and standard orientation programs; address the need for adequate resources; and coordinate strategies for working consistently with law enforcement and first responders in remote areas of the country. As of December 2006, all but two recommendations have been closed.

Follow-up on the FBI's Progress Toward Biometric Interoperability Between Fingerprint Systems

In July 2006, the OIG issued the latest of six reports monitoring the FBI's progress toward achieving biometric interoperability between the FBI's Integrated Automated Fingerprint Identification System (IAFIS) and the DHS Automated Biometric Identification System (IDENT). Fully interoperable fingerprint systems would allow law

enforcement and immigration officers to more readily identify criminals and known or suspected terrorists trying to enter the United States, as well as to identify those already in the United States. The OIG found that the FBI and the DHS are moving forward toward interoperability and developing the first phase of a three-phase plan to make IDENT and IAFIS fully interoperable by December 2009.

In the first phase, the agencies plan to deploy a joint automated system for near real-time (updated within 24 hours) sharing of certain key immigration and law enforcement data between the FBI and the DHS by September 3, 2006. In the remaining two phases, the FBI and the DHS plan to expand the data shared to include law enforcement and immigration data in IAFIS and IDENT, and to allow access to that data by federal, state, and local law enforcement agencies, authorized non-criminal justice agencies, and immigration authorities. By December 2009, users of the two systems are expected to be able to submit a single request that searches all fingerprint records maintained by the FBI and the DHS to receive associated criminal history and immigration information about the subject.

To support full interoperability, the FBI is upgrading IAFIS to process more flat (in lieu of rolled) fingerprint submissions, and the DHS is planning to modernize IDENT and convert its entry/exit and border security system, US-VISIT, from a 2- to a 10-fingerprint system. The FBI and the DHS have identified technical, funding, and policy risks to achieving full interoperability; have developed risk mitigation strategies; and are working to estimate the costs for the second interoperability phase.

Until a fully interoperable system is available, the FBI has taken interim actions to lessen the risk that criminal aliens or terrorists will enter the United States undetected. These include providing daily transmissions of key terrorist records to the DHS, improving overall IAFIS availability and capacity for DHS fingerprint searches, and reducing the response time to DHS requests for checks of aliens' fingerprints.

Examples of Recent Investigations Division Cases

False Statements

An investigation by the OIG's Dallas Field Office determined that a former FBI Special Agent in Charge (SAC) concealed material facts from the FBI regarding his association with the Mexican national allegedly involved in money laundering and drug trafficking and made false statements in Office of Government Ethics Public Financial Disclosure Reports submitted to the FBI for 2002 and 2003 regarding gifts totalling over \$100,000 allegedly received from the Mexican national. The SAC was employed by the FBI for 23 years and served as the SAC of the El Paso Division from July 2001 to November 2003. He retired from the FBI on November 7, 2003, 2 days after his OIG interview. In August 2006, the former SAC was convicted in the Western District of Texas on two counts of a five-count indictment charging him with making false statements. On January 5, 2007, the former SAC was sentenced to 6 months' incarceration and 3 years' supervised release. He was also ordered to pay a \$10,000 fine and perform 200 hours of community service.

Fraud

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

Theft

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

Bribery

An investigation by the OIG's Philadelphia Area Office led to the arrest and guilty plea of a BOP senior correctional officer assigned to the Federal Detention Center in Philadelphia, Pennsylvania, to charges of bribery. The OIG investigation determined that the officer procured cell phones, supplies, drugs, and other contraband for several prisoners in exchange for bribe payments in excess of \$12,000. The officer was sentenced to 1 year incarceration and 3 years' supervised release, and ordered to pay a \$15,000 fine.

Embezzlement An investigation by the OIG's Miami Field Office led to the arrest of a DEA special agent on charges of converting property of another, embezzlement of public funds, and money laundering. An indictment returned in the Northern District of Georgia alleged that the special agent, who served as a team leader and evidence custodian at the DEA's Atlanta Airport Task Force from early 2003 to January 2005, embezzled cash seized from money couriers for drug organizations by instructing local police officers to turn over seized money to him without counting it. The special agent allegedly stole more than \$200,000, and used a portion of the embezzled money to build a custom home in Orlando, Florida.

Bid Rigging

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

PERFORMANCE AND RESOURCES 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.										
WORKLOAD/RESOURCES	Final Target		Actual		Estimate		Changes		Requested (Total)	
	FY 2006		FY 2006		FY 2007		Current Services Adjustments & FY 2008 Program Changes*		FY 2008 Request	
	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000
Total Costs and FTE										
(reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)	449	\$67,096	459	\$69,852	-11	\$3,356	448	\$73,208
		[\$15,219]		[\$18,282]		[\$1,220]		[\$19,502]
Performance Report and Performance Plan										
Workload **										
Number of Cases Opened per 1,000 DOJ employees:										
Fraud		**	0.42		**		**		**	**
Bribery		**	0.61		**		**		**	**
Rights Violations		**	0.27		**		**		**	**
Sexual Crimes		**	0.32		**		**		**	**
Official Misconduct		**	1.27		**		**		**	**
Theft		**	0.20		**		**		**	**
Output										
Investigations closed		447	441		447		1		448	
Integrity Briefings and Presentations to DOJ employees***		130	202		140		0		140	
DOJ employees attending Integrity Briefings***		4,000	9,308		4,200		0		4,200	
** Beginning with FY 2006, these workload numbers will be reported only as actuals. This information was never intended as targets, but to provide "trend" information over time.										
*** The FY 2007 target has changed to reflect an expected increase in employees attending Integrity Briefings.										

* The OIG's increases are due to Program Changes (\$460) and not Current Services Adjustments (\$2,896).

PERFORMANCE AND RESOURCES 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.										
WORKLOAD/RESOURCES	Final Target		Actual		Estimate		Changes		Requested (Total)	
	FY 2006		FY 2006		FY 2007		Current Services Adjustments & FY 2008 Program Changes*		FY 2008 Request	
	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000
Total Costs and FTE										
(reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)	449	\$67,096	459	\$69,852	-11	\$3,356	448	\$73,208
		[\$15,219]		[\$18,282]		[\$1,220]		[\$19,502]
Performance Report and Performance Plan										
Intermediate Outcome										
Percentage of Investigations closed or referred for prosecution within 1 year		75%		72%		75%		0%		75%
Number of closed Investigations substantiated **		**		239		**		**		**
Arrests **		**		134		**		**		**
End Outcome										
Convictions **		**		112		**		**		**
Administrative Actions **		**		175		**		**		**
Response to Customer Surveys:										
Report completed in a timely manner (%)		90%		97%		90%		0%		90%
Issues were sufficiently addressed (%)		90%		99%		90%		0%		90%
** Indicators for which the OIG only reports actuals.										

* The OIG's increases are due to Program Changes (\$460) and not Current Services Adjustments (\$2,896).

PERFORMANCE/RESOURCES TABLE (Goal 1)

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.

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 new computer-based relational database system that became operational at the end of June 2005. Most of the legacy data was converted except for records older than FY 1993, which were archived. We are developing new reports to run against the database and verifying the accuracy of the conversion. We will rerun the new reports against historical data and also compare them with historical reports to validate the results and to audit the data. The database administrator also will run 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 and transaction log backups are scheduled nightly and in 3 hour intervals. The data consistency checker, index tuning, and alerts are to be scheduled weekly.

Investigations Division Monthly Investigative Activity Report – Most of the data for this report was designed into the new IDMS application, except for integrity briefing activities and the use of certain investigative techniques. The field offices enter most data into IDMS and separately submit their integrity briefing activities and the use of mail covers, handwriting analysis, and some forms of electronic intercepts.

Investigations Division Administrative Database - a new 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 2006 Performance Report:

In general, most targets were met or exceeded. The ones not met, particularly the number of investigations closed and the percentage of investigations closed or referred for prosecution within 1 year, were not met due to the higher than usual number of complex cases.

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 2000	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006		FY 2007	FY 2008
	Actual	Actual	Actual	Actual	Actual	Actual	Target	Actual	Target	Target
Workload										
Number of Cases Opened per 1,000 DOJ employees:										
Fraud	N/A	N/A	1.33	0.97	0.59	0.52	*	0.42	*	*
Bribery	N/A	N/A	1.61	1.63	0.75	0.58	*	0.61	*	*
Rights Violations	N/A	N/A	0.36	0.38	0.19	0.31	*	0.27	*	*
Sexual Crimes	N/A	N/A	0.56	0.86	0.44	0.41	*	0.32	*	*
Official Misconduct	N/A	N/A	1.38	1.63	1.06	1.03	*	1.27	*	*
Theft	N/A	N/A	N/A	N/A	N/A	0.18	*	0.2	*	*
Output										
Investigations closed	608	590	606	607	486	415	447	441	447	448
Integrity Briefings and Presentations to DOJ employees	62	126	209	107	183	235	130	202	140	140
DOJ employees attending Integrity Briefings	1,735	3,699	6,286	4,601	8,287	11,239	4,000	9,308	4,200	4,200
Intermediate Outcome										
Percentage of Investigations closed or referred for prosecution within 1 year	N/A	N/A	80%	65%	66%	66%	75%	69%	75%	75%
Number of closed Investigations substantiated	135	157	179	194	165	180	**	239	**	**
Arrests	149	159	209	192	106	69	**	134	**	**
End Outcome										
Convictions	120	139	150	165	124	66	**	112	**	**
Administrative Actions	118	175	161	175	137	154	**	175	**	**
Response to Customer Surveys:										
Report completed in a timely manner (%)	N/A	N/A	99%	98%	93%	94%	90%	97%	90%	90%
Issues were sufficiently addressed (%)	N/A	N/A	100%	98%	95%	91%	90%	99%	90%	90%

* Beginning with FY 2006, these workload numbers will be reported only as actuals. This information was never intended as targets, but to provide "trend" information over time.

** Indicators for which the OIG only reports actuals.

PERFORMANCE AND RESOURCES 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.										
WORKLOAD/RESOURCES	Final Target		Actual		Estimate		Changes		Requested (Total)	
	FY 2006		FY 2006		FY 2007		Current Services Adjustments & FY 2008 Program Changes*		FY 2008	
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)	449	\$67,096	459	\$69,852	-11	\$3,356	448	\$73,208
		[\$15,219]		[\$18,282]		[\$1,220]		[\$19,502]
Performance Report and Performance Plan										
Workload										
Assignments initiated**		132		118		134		1		135
Percent of technical CSITAO resources devoted to security reviews of major Dept. information systems		75%		86%		86%		0%		86%
Percent of internal audit assignments that assess component performance measures		10%		11%		10%		0%		10%
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**		75%		85%		78%		0%		78%
Intermediate Outcome										
Assignments completed**		131		114		133		1		134

* The OIG's increases are due to Program Changes (\$460) and not Current Services Adjustments (\$2,896).

** FY 2007 targets changed to better align with resources.

PERFORMANCE AND RESOURCES 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.										
WORKLOAD/RESOURCES	Final Target		Actual		Estimate		Changes		Requested (Total)	
	FY 2006		FY 2006		FY 2007		Current Services Adjustments & FY 2008 Program Changes*		FY 2008 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)	449	\$67,096	459	\$69,852	-11	\$3,356	448	\$73,208
		[\$15,219]		[\$18,282]		[\$1,220]		[\$19,502]
Performance Report and Performance Plan										
Intermediate Outcome										
Percent of Audit resources devoted to reviews of grants and grant management		25%		28%		25%		0%		25%
Components receiving information system audits		5		4		5		0		5
Products issued to the Dept. containing significant findings or information for management decision-making**		105		97		102		1		103
Products issued to Congress**		47		46		45		1		46
Percent of E&I assignments completed within the timeframes established by the IG.		70%		64%		70%		0%		70%
Percent of contract, grant, IGA, and other external audits to be completed in draft within 5 months		60%		51%		60%		0%		60%
Percent of internal audits to be completed within 1 year		60%		68%		60%		0%		60%

* The OIG's increases are due to Program Changes (\$460) and not Current Services Adjustments (\$2,896).

** The FY 2007 targets changed to better align with resources.

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 2006 Performance Report:

Targets not met are largely due to other reviews being conducted that included Internal Management Reviews, Internal and External Peer Reviews, and new evaluation work processes.

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 2000	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006		FY 2007	FY 2008
	Actual	Actual	Actual	Actual	Actual	Actual	Target	Actual	Target	Target
Workload										
Assignments initiated	300	213	266	227	140	118	132	118	134	135
Percent of Evaluation and Inspections (E&I) workdays devoted to follow-up reviews	25%	5%	16%	19%	N/A	N/A	N/A	N/A	N/A	N/A
Percent of technical CSITAO resources devoted to security reviews of major Dept. information systems	82%	94%	79%	48%	51%	100%	75%	86%	86%	86%
Percent of internal audit assignments that assess component performance measures	3%	18%	66%	32%	13%	10%	10%	11%	10%	10%
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	N/A	N/A	62%	55%	76%	92%	75%	85%	78%	78%
Intermediate Outcome										
Assignments completed*	487	270	253	233	123	139	131	114	133	134
Percent of Audit resources devoted to reviews of grants and grant management	N/A	N/A	24%	20%	38%	33%	25%	28%	25%	25%
Components receiving information system audits	6	6	8	7	5	6	5	4	5	5
Products issued to the Dept. containing significant findings or information for management decision-making*	484	103	251	233	124	122	105	97	102	103
Products issued to Congress	41	37	50	44	51	51	47	46	45	46
Percent of E&I assignments to be completed within 6 months	N/A	N/A	66%	50%	27%	78%	70%	64%	70%	70%
Percent of contract, grant, IGA, and other external audits to be completed within 5 months	N/A	N/A	89%	81%	71%	68%	60%	51%	60%	60%
Percent of internal audits to be completed within 1 year	N/A	N/A	83%	65%	43%	59%	60%	68%	60%	60%

* Beginning in 2001, the decrease reflects the termination of the OIG's agreement with the Executive Office for U.S. Trustees to conduct performance audits on Chapter 7 trustees.

3. 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 its work. 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, as well as for cross-cutting work that covers multiple components, such as the OIG's recent reviews of component's disciplinary programs or their handling of shooting incidents. 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 Challenges.

Program Increases

Item Name: Counterterrorism Oversight

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

Component Ranking of Item: **1** of **1**

Program Increase: Positions **+5** Agt/Atty **+1**.....FTE **+3** Dollars **+\$460**

Description of Item

The OIG is requesting 3 auditors, 1 program analyst, and 1 attorney for Counterterrorism Oversight.

Justification

Specifically, the requested positions would be deployed in the following area:

Preventing and Combating Terrorism

As funding for the Department's counterterrorism efforts continues to increase, so does the need to monitor and evaluate Department programs to identify possible vulnerabilities. This request will enable the OIG to assist the Department in ensuring that its counterterrorism funds are put to the most effective use.

The FBI has established as its highest priority the prevention of terrorist attacks on the United States. The accomplishment of this critical national security mission requires the FBI to collect, analyze, and appropriately disseminate intelligence and other information needed to disrupt or defeat terrorist activities. However, in the past congressional investigations and OIG reports have found weaknesses in the FBI's ability to effectively carry out these vital efforts. Given the importance of the FBI's counterterrorism mission, the additional requested positions will enable the OIG to expand its oversight program in the FBI.

With these positions, the OIG will continue to examine key issues in the FBI, including development of its Sentinel Case Management System, its efforts to protect the nation's seaports, and its process for reporting possible violations involving its intelligence activities to the President's Intelligence Oversight Board. The OIG will continue to conduct audits and reviews on topics such as the operations of the Terrorist Screening Center, the Department's Internal Controls over Terrorism Reporting, Intelligence Sharing, and the Bureau of Prisons' efforts to improve the monitoring of communications for terrorists and other high-risk inmates.

Additional resources would enable the OIG to undertake new reviews in these and other critical areas.

Impact on Performance (Relationship of Increase to Strategic Goals)

All personnel requests are in direct support of the Department's Strategic Goals and Objectives. The OIG is a key player in meeting the Department's Strategic Goals and Objectives by providing leadership in integrity, efficiency and effectiveness, and management excellence. See the performance indicator charts for the description of the OIG's general goals and the performance effect of the FY 2008 enhancements.

Funding
(Dollars in Thousands)

Base Funding

FY 2006 Enacted				FY 2007 Estimate				FY 2008 President's Budget Current Services			
Pos	Agt/ Atty	FTE	\$(000)	Pos	Agt/ Atty	FTE	\$(000)	Pos	Agt/ Atty	FTE	\$(000)

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 2008 Request (\$000)
Attorney (GS-15)	120	1	120
Program Analyst (GS-14)	90	1	90
Auditor (GS-14)	90	1	90
Auditor (GS-13)	80	2	160
Total Personnel		5	\$460

Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2008 Request
Not Applicable	0	0	\$0
Total Non-Personnel	0	0	\$0

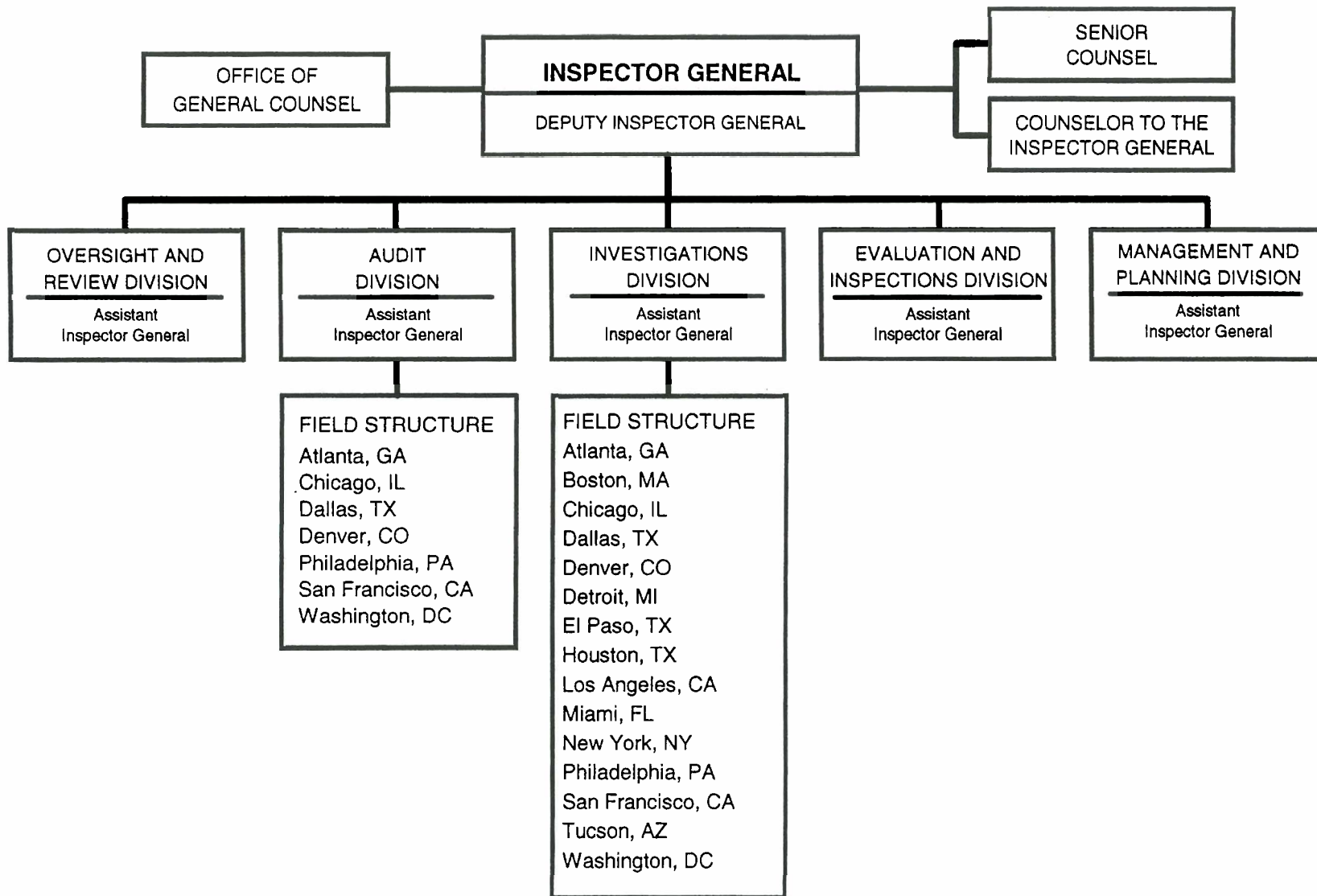
Total Request for This Item

	Pos	Agt/Atty	FTE	Personnel	Non-Personnel	Total
Current Services	-	-	-	-	-	-
Increases	5	0/1	3	\$460	\$0	\$460
Grand Total	5	0/1	3	\$460	\$0	\$460

Program Offsets
(Not Applicable)

V. EXHIBITS

OFFICE OF THE INSPECTOR GENERAL



Approved by: Glenn A Fine

Date: 5/10/06

B. Summary of Requirements

Summary of Requirements
OFFICE OF THE INSPECTOR GENERAL
Salaries and Expenses
(Dollars in thousands)

	FY 2008 Pres. Budget		
	Perm. Pos.	FTE	Amount
2006 Enacted (with Rescissions, direct only)	449	427	67,922
Total 2006 Enacted (with Rescissions and Supplementals)	449	427	67,922
2007 President's Budget (Information Only)	449	459	70,558
2007 Continuing Resolution Level (as reflected in the 2008 President's Budget; Information Only)	449	459	67,922
2007 Estimate (direct only)*	449	437	69,852
2007 Estimate (with Rescissions)	449	437	69,852
Technical Adjustments (Reimbursable)	1 1/	...
Adjustments to Base			
Increases:			
2008 Pay Raise (3.0%)	1,033
2007 Pay Raise Annualization (2.2%)	360
Change in Compensable Days	380
Thrift Savings Plan (TSP)	110
Health Insurance	136
Employees Compensation Fund	56
General Services Administration (GSA) Rent	137
Department of Homeland Security (DHS) Security Charges	48
Moves (Lease Expirations)	558
Security Investigations	78
Subtotal Increases	2,896
Decreases:			
Unfunded Position and FTE Reduction	-15	-15	...
Total Adjustments to Base	-15	-15	2,896
Total Adjustments to Base and Technical Adjustments	-15	-14	2,896
2008 Current Services (Direct)	434	422	72,748
Program Changes			
Increases:			
Counterterrorism Oversight	5	3	460
Subtotal Increases	5	3	460
Total Program Changes	5	3	460
2008 Total Request (Direct)	439	425	73,208
2007 - 2008 Total Change (Direct)	-10	-12	3,356

* The Department's 2008 budget request was built on a starting point that recognized progress in enacting the FY 2007 appropriation. The starting point used (referred to throughout this document as the "Estimate") is the average of the Senate Committee and House passed marks, less one percent, unless noted otherwise.

1/ Reimbursable FTE increased by 1 in FY 2008 due to additional Federal Information Security Management Act (FISMA) Audit work in FY 2007.

B. Summary of Requirements

Summary of Requirements
OFFICE OF THE INSPECTOR GENERAL
Salaries and Expenses
(Dollars in thousands)

	2006 Enacted w/ Rescissions and Supplementals			2007 Estimate			2008 Adjustments to Base and Technical Adjustments			2008 Current Services			2008 Increases			2008 Offsets			2008 Request		
	Pos.	FTE	Amount	Pos.	FTE	Amount	Pos.	FTE	Amount	Pos.	FTE	Amount	Pos.	FTE	Amount	Pos.	FTE	Amount	Pos.	FTE	Amount
Audits, Inspections, Investigations, and Reviews	449	427	\$67,922	449	437	\$69,852	-15	-15	\$2,896	434	422	\$72,748	5	3	\$460	439	425	\$73,208
Reimbursable FTE		<u>22</u>			<u>22</u>			1			<u>23</u>									<u>23</u>	
Total FTE		449			459						445									448	
Other FTE:																					
LEAP		21			21						21									21	
Overtime		<u>2</u>			<u>2</u>						<u>2</u>									<u>2</u>	
Total Compensable FTE		472			482						468									471	

Note: Reimbursable FTE increased by 1 in FY 2008 due to additional FISMA Audit work in FY 2007.

C: Program Increases/Offsets by Decision Unit

FY 2008 Program Increases/Offsets by Decision Unit
OFFICE OF THE INSPECTOR GENERAL
Salaries and Expenses
(Dollars in thousands)

Program Increases	Location of Description by Decision Unit	Decision Unit				Total Increases
		Pos.	Agent/Attorney	FTE	Amount	
Counterterrorism Oversight	See note below.	5	0/1	3	\$460	\$460
Total Program Improvements		5	0/1	3	\$460	\$460

Program Offsets	Location of Description by Decision Unit	Decision Unit				Total Offsets
		Pos.	Agent/Attorney	FTE	Amount	
None	See note below.

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

D. Resources by DOJ Strategic Goal and Strategic Objective

Resources by Department of Justice Strategic Goal/Objective
OFFICE OF THE INSPECTOR GENERAL
Salaries and Expenses
(Dollars in thousands)

Strategic Goal and Strategic Objective	2006 Appropriation Enacted w/Rescissions and Supplementals		2007 Estimate		2008 Current Services		2008 Increases		2008 Offsets		2008 Request	
	Direct, Reimb. Other FTE	Direct Amount	Direct, Reimb. Other FTE	Direct Amount	Direct, Reimb. Other FTE	Direct Amount	Direct, Reimb. Other FTE	Direct Amount	Direct, Reimb. Other FTE	Direct Amount	Direct, Reimb. Other FTE	Direct Amount
All Department Goals and Objectives*	449	67,922	459	69,852	445	72,748	3	460	448	73,208
Grand Total	449	67,922	459	69,852	445	72,748	3	460	448	73,208

* The OIG helps the Department pursue its Strategic Goals and Objectives through the OIG's investigations, audits, inspections, and program reviews.

E. Justification for Base Adjustments

Justification for Base Adjustments
Office of the Inspector General
Salaries and Expenses
(Dollars in Thousands)

<u>Increases</u>	<u>Pos.</u>	<u>FTE</u>	<u>Amount</u>
1. <u>2008 Pay Raise</u> This request provides for the proposed 3.0 percent pay raise to be effective in January 2008. This increase includes locality pay adjustments as well as the general pay raise. The amount requested, <u>\$1,033,000</u> , represents the pay amounts for three-quarters of the fiscal year plus appropriate benefits (<u>\$775,000</u> for pay and <u>\$258,000</u> for benefits).	\$1,033
2. <u>Annualization of 2007 Pay Raise</u> This pay annualization represents first quarter amounts (October through December) of the 2007 pay increase of 2.2 percent. The amount requested <u>\$360,000</u> , represents the pay for one-quarter of the fiscal year plus appropriate benefits (<u>\$270,000</u> for pay and <u>\$90,000</u> for benefits).	360
3. <u>Change in Compensable Days</u> The increased costs of two more compensable days in FY 2008 compared to FY 2007 is calculated by dividing the FY 2007 estimated personnel compensation <u>\$39,768,000</u> and applicable benefits <u>\$9,620,000</u> by 260 compensable days. The cost increase of two compensable days is <u>\$380,000</u>	380
4. <u>Thrift Savings Plan</u> The cost of agency contributions to the Thrift Savings Plan will also rise as FERS participation increases. The contribution rate is 4.3 percent and the increase of the TSP is <u>\$110,000</u>	110
5. <u>Health Insurance</u> Effective January 2006, the OIG's contribution to Federal employees' health insurance premiums increased by <u>6.9</u> percent. Applied against the 2007 estimate of <u>\$1,841,000</u> , the additional amount required for FY 2008 is <u>\$136,000</u>	136
6. <u>Employees Compensation Fund</u> This item reflects an increase of <u>\$56,000</u> for the estimated billing from the Department of Labor for costs in 2006 of employees' accident compensation, which will be billed in 2008.	56
7. <u>General Services Administration (GSA) Rent</u> GSA will continue to charge rental rates that approximate those charged to commercial tenants for equivalent space and related services. The requested increase of <u>\$137,000</u> is required to meet our commitment to GSA. The costs associated with GSA rent were derived through the use of an automated system, which uses the latest inventory data, including rate increases to be effective in FY 2007 for each building currently occupied by Department components, as well as the costs of new space to be occupied. GSA provided data on the rate increases.	137

E. Justification for Base Adjustments

Justification for Base Adjustments
Office of the Inspector General
Salaries and Expenses
(Dollars in Thousands)

<u>Increases</u>	<u>Pos.</u>	<u>FTE</u>	<u>Amount</u>
8. <u>DHS Security Charges</u> The DHS will continue to charge Basic Security and Building Specific Security. The requested increase of <u>\$48,000</u> is required to meet our commitment to DHS and cost estimates that were developed by DHS.	48
9. <u>Moves (Lease Expirations)</u> GSA requires all agencies to pay relocation costs associated with lease expirations. This request provides for the costs associated with new office relocations caused by the expiration of leases in FY 2008. Funding of <u>\$558,000</u> is required for this account.	558
10. <u>Security Investigations</u> The <u>\$78,000</u> increase reflects payments to the Office of Personnel Management for security reinvestigations for employees requiring security clearances.	78
 <u>Total Increases</u>		 \$2,896
<u>Decreases:</u>			
Unfunded Position and FTE Reduction	-15	-15	...
<u>Total Adjustments to Base</u>	-15	-15	\$2,896

Note: ATBs must be recalculated following final FY 2007 action.

F. Crosswalk of 2006 Availability

Crosswalk of 2006 Availability
OFFICE OF THE INSPECTOR GENERAL
Salaries and Expenses
(Dollars in thousands)

Decision Unit	FY 2006 Enacted Without Rescission			Rescissions			Supplementals			Reprogrammings/ Transfers			Carryover/ Recoveries			2006 Availability		
	Pos.	FTE	Amount	Pos.	FTE	Amount	Pos.	FTE	Amount	Pos.	FTE	Amount	Pos.	FTE	Amount	Pos.	FTE	Availability
Audits, Inspections, Investigations, and Reviews	454	432	\$68,801	-5	-5	-\$879	449	427	\$67,922
Reimbursable FTE		22															22	
Total FTE		454															449	
Other FTE																		
LEAP		21															21	
Overtime		2															2	
Total Compensable FTE		477															472	

Enacted Rescissions: \$193,000 was rescinded by P.L. 109 -108 and \$686,000 was rescinded by P.L. 109 -148 for a total of \$879,000.

G. Crosswalk of 2007 Availability

Crosswalk of 2007 Availability
OFFICE OF THE INSPECTOR GENERAL
Salaries and Expenses
(Dollars in thousands)

Decision Unit	FY 2007 Estimate			Rescissions			Reprogrammings/ Transfers			Unobligated Balances Carried Forward/Recoveries			2007 Availability		
	Pos.	FTE	Amount	Pos.	FTE	Amount	Pos.	FTE	Amount	Pos.	FTE	Amount	Pos.	FTE	Availability
Audits, Inspections, Investigations, and Reviews	449	437	\$69,852	449	437	\$69,852
Reimbursable FTE		22												22	
Total FTE		459												459	
Other FTE															
LEAP		21												21	
Overtime		2												2	
Total Compensable FTE		482												482	

H: Summary of Reimbursable Resources

Summary of Reimbursable Resources
OFFICE OF THE INSPECTOR GENERAL
Salaries and Expenses

(Dollars in thousands)

Collections by Source	2006 Enacted			2007 Planned			2008 Request			Increase/Decrease		
	Pos.	FTE	Amount	Pos.	FTE	Amount	Pos.	FTE	Amount	Pos.	FTE	Amount
Financial Statement Audits	16	16	13,073	16	16	15,504	16	16	16,702	1,198
FISMA	6	6	2,146	7	7	2,778	7	7	2,800	22
Budgetary Resources:	22	22	\$15,219	23	23	\$18,282	23	23	\$19,502	\$1,220
<u>Obligations by Program:</u>												
Audit, Investigations, Evaluation & Inspections	22	22	\$15,219	23	23	\$18,282	23	23	\$19,502	\$1,220

Note: Reimbursable FTE increased by 1 in FY 2007 due to additional FISMA Audit work.

Financial Statement Audits (FSA) - In accordance with the Chief Financial Officers Act and the Government Management Reform Act, the OIG oversees the FSA for all audited accounts within the Department.

Federal Information Security Management Act (FISMA) - FISMA requires an annual independent evaluation of each agency's information security program and practices. The OIG reviewed five systems in FY 2006 and projects it will review five systems in FY 2007 and five systems in FY 2008.

I. Detail of Permanent Positions by Category

Detail of Permanent Positions by Category
OFFICE OF THE INSPECTOR GENERAL
Salaries and Expenses

Category	2006 Enacted w/ Rescissions and Supps		2007 Estimate		2008 Request					
	Total Authorized	Total Reimbursable	Total Authorized	Total Reimbursable	ATBs	Program Increases	Program Decreases	Total Program Changes	Total Authorized	Total Reimbursable
Personnel Management [200-299].....	8	...	8	8	...
General Admin. & Clerical [300-399].....	148	3	148	3	-12	1	...	1	137	3
Accounting & Budget [500-599].....	108	14	108	14	-3	3	...	3	108	15
Attorneys [905].....	24	...	24	1	...	1	25	...
Paralegal [950, 986]	2	...	2	2	...
Operations Research Analyst [1515]...	2	...	2	2	...
Investigative Analyst [1801]	7	...	7	7	...
Investigative Assistants [1802].....	2	...	2	2	...
Criminal Investigations Series [1811].....	135	...	135	135	...
Information Tech Specialist [2210].....	13	5	13	5	13	5
Total	449	22	449	22	...	5	...	5	439	23
Headquarters (Washington, D.C.).....	220	22	220	22	-8	2	...	2	214	23
U.S. Field.....	229	...	229	...	-7	3	...	3	225	...
Foreign Field
Total	449	22	449	22	-15	5	...	5	439	23

Note: The position requested in the "General Admin & Clerical [300-399]" category represents a Program Analyst (343 series) position. Reimbursable FTE increased by 1 in FY 2008 due to additional FISMA Audit work in FY 2007.

J: Financial Analysis of Program Changes

Financial Analysis of Program Changes OFFICE OF THE INSPECTOR GENERAL Salaries and Expenses (Dollars in Thousands)

	Counterterrorism Oversight		Program Changes	
	Pos.	Amount	Pos.	Amount
Grades:				
GS-15	1	143	1	143
GS-14	2	192	2	192
GS-13.....	2	162	2	162
Total Positions & Annual Rate.....	5	497	5	497
Lapse (-).....	-3	-249	-3	-249
Other Compensation LEAP.....	[...]	...	[...]	...
Total FTE & Personnel Compensation.....	3	249	3	249
Personnel benefits		75		75
Travel & Transportation.....		26		26
Comm., Util., Other.....		7		7
GSA Rent
Print/Reproduction.....	
Advisory & Assistance Services		3		3
Other Services.....		30		30
Purchase of Goods & Svc from Gov't Act.		24		24
Supplies and materials.....		14		14
Equipment.....		32		32
Total, 2008 Program Changes Requested	3	460	3	460

Note: Totals may not add due to rounding.

K. Summary of Requirements by Grade

**Summary of Requirements by Grade
OFFICE OF THE INSPECTOR GENERAL
Salaries and Expenses**

Grades and Salary Ranges	2006 Actual		2007 Estimate		2008 Request		Increase/Decrease	
	Pos.	Amount	Pos.	Amount	Pos.	Amount	Pos.	Amount
EX, \$136,200-186,600	1		1		1	
SES, \$111,676 - 168,000	7		7		7	
SL, \$111,676-154,600	2		2		2	
GS-15, \$110,363-143,471	60		60		61		...	1
GS-14, \$93,822-121,967	77		77		79		...	2
GS-13, \$79,397-103,220	208		208		195		...	-13
GS-12, \$66,767-86,801	34		34		34	
GS-11, \$55,706-72,421	13		13		13	
GS-10, \$50,703-65,912	1		1		1	
GS-9, \$46,041-59,852	22		22		22	
GS-8, \$41,686-54,194	10		10		10	
GS-7, \$37,640-48,933	14		14		14	
Total, Appropriated Positions	449		449		439		...	-10
Average SES Salary		\$151,549		\$155,641		\$160,310		
Average GS Salary		\$78,478		80,550		\$83,138		
Average GS Grade		12.80		12.80		12.80		

L. Summary of Requirements by Object Class

Summary of Requirements by Object Class OFFICE OF THE INSPECTOR GENERAL Salaries and Expenses

(Dollars in thousands)

Object Class	2006 Actual Obligations		2007 Estimate		2008 Request		Increase/Decrease	
	FTE	Amount	FTE	Amount	FTE	Amount	FTE	Amount
11.1 Total FTE & personnel compensation	403	33,459	413	35,778	401	37,380	-12	1,602
11.3 Other than full-time permanent	24	534	24	534	24	534	0	0
11.5 Other personnel compensation	23	502	23	502	23	502	0	0
Overtime	[2]	6	[2]	35	[2]	37	0	2
Law Enforcement Availability Pay	[21]	2,772	[21]	2,858	[21]	2,945	[0]	87
11.8 Special personal services payments	0	10	0	5	0	15	0	10
Total	450	37,283	460	39,712	448	41,413	-12	1,701
Reimbursable FTE:								
Full-time permanent	[22]		[22]		[23]		[1]	
Other Object Classes:								
12.0 Personnel benefits		11,237		11,565		12,263		698
12.1 Transit subsidy		195		200		200		0
13.0 Benefits to former personnel		6		24		24		0
21.0 Travel and transportation of persons		3,545		3,520		3,546		26
22.0 Transportation of things		307		130		130		0
23.1 GSA rent		7,793		8,549		9,292		743
23.3 Comm., util., & other misc. charges		1,511		1,495		1,502		7
24.0 Printing and reproduction		28		31		31		0
25.1 Advisory and Assistance services		1,038		1,054		1,057		3
25.2 Other Services		1,458		1,453		1,483		30
25.3 Purchases of goods & svc from Gov't accounts		985		943		1,045		102
25.4 Operation & Maintenance of Facilities		32		32		32		0
25.6 Medical Care		34		90		90		0
26.0 Supplies and materials		386		393		407		14
31.0 Equipment		1,253		641		673		32
42.0 Claims & Indemnities		5		20		20		0
Total obligations		67,096		69,852		73,208		3,356
Unobligated balance, start of year	
Unobligated balance, end of year		826	
Recoveries of prior year obligations	
Total requirements		67,922		69,852		73,208		3,356
Relation of Obligations to Outlays:								
Total obligations		67,096		69,852		73,208		
Obligated balance, start of year		6,065		8,160		10,575		
Obligated balance, end of year		(8,160)		(10,575)		(11,305)		
Recoveries of prior year obligations		-669			
Outlays		64,332		67,437		72,478		

Note: Reimbursable FTE increased by 1 in FY 2008 due to increased FISMA Audit work in FY 2007.

M. Status of Congressionally Requested Studies, Reports, and Evaluations

1. In accordance with the requirements of the Department's FY 2006 Appropriations Conference Report, the OIG was directed to provide an inventory of major Department IT systems and report on research, plans, studies, and evaluations that the Department has produced, or is in the process of producing, concerning its information systems. In response, the OIG issued the first of three reports in March 2006: A report of the Department's major IT system investments by investment title/component, investment description, implementation status, and actual and projected costs. The second report will provide an audited verification of the information detailed in the unaudited report. The third report will detail the Department's research, plans, studies, and evaluations along with an analysis identifying the depth and scope of the problems the Department has experienced in the formulation of its IT plans. We plan to issue the second and third reports by mid-2007.

2. The Conference Report associated with the FY 2006 Department of Justice Appropriations Act directed the OIG to provide the Committees on Appropriations with regular updates during fiscal year 2006 on the financial and programmatic status of SENTINEL. The OIG will continue to provide updates in FY 2007 and throughout the life of the project.

3. The Conference Report associated with the FY 2006 Department of Justice Appropriations Act directed the OIG to review and assess how well the investigations conducted by the DEA's Mobile Enforcement Teams, the FBI's Safe Street Task Forces, the USMS's Fugitive Task Forces, and ATF's Violent Crimes Impact Teams are coordinated. The target date for submission is Spring 2007.