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

1. **Counterterrorism**: The most critical challenge the Department of Justice (Department) continues to face is the ongoing effort to deter and disrupt acts of terrorism. This has been the Department's highest priority since the terrorist attacks of September 11, 2001. Five years later, the Department has substantially enhanced its counterterrorism capabilities, but its counterterrorism efforts still remain a top challenge in need of continued improvement.

   The most significant changes in the Department's counterterrorism efforts during the past 5 years involve the Federal Bureau of Investigation's (FBI) transformation into a more proactive, intelligence-driven agency dedicated to preventing acts of terrorism rather than primarily a law enforcement agency focused on investigating crimes after they have occurred. In its most recent reorganization, announced in July 2006, the FBI created an organizational structure of five branches that reflects its new counterterrorism priority: National Security, Criminal Investigations, Science and Technology, Office of the Chief Information Officer, and Human Resources. The National Security Branch consists of the FBI's Counterterrorism and Counterintelligence Divisions, Directorate of Intelligence, and Weapons of Mass Destruction Directorate.

   Since the September 11 attacks, the FBI led the effort to create the Terrorist Screening Center (TSC), a multi-agency effort designed to consolidate information on domestic and international terrorists and provide 24-hour, 7-day a week responses for screening individuals against the consolidated terrorist watch list. Prior to establishment of the TSC, the federal government relied on more than a dozen separate watch lists maintained by a variety of federal agencies to search for terrorist-related information about individuals who, for example, apply for a visa, attempt to enter the United States through a port of entry, attempt to travel internationally on a commercial airline, or are stopped by a local law enforcement officer for a traffic violation.

   In addition, in 2005 the FBI created a Directorate of Intelligence to manage its expanded intelligence program. As part of that effort, the FBI has increased the size of its analytical corps from 1,023 analysts in October 2001 to 2,161 analysts in September 2006 – a net increase of 1,138 intelligence analysts or 111 percent – and the FBI has placed intelligence analysts in each of its 56 domestic field offices.

   As we discuss in more detail in the challenge relating to violent crime, after the September 11 attacks the FBI reallocated significant agent and analyst resources from traditional criminal investigations, such as drug trafficking, health care fraud, and financial crimes, to counterterrorism and counterintelligence matters. These shifts present management challenges not only for the FBI, which continues to have responsibility for traditional criminal matters, but also for other federal, state, and local law enforcement organizations affected by the FBI's reduced involvement in certain criminal investigations. For example, an Office of the Inspector General (OIG) review of the effects of the FBI's reallocation of resources found that the FBI opened 28,331 fewer criminal cases in fiscal year (FY) 2004 than it had in FY 2000, a 45-

percent reduction. Each of the FBI's criminal programs experienced fewer case openings during this period, including a 47-percent reduction in Violent Crimes and a 40-percent reduction in Financial Crimes. The FBI's greatest reduction occurred in drug-related investigations, with 70 percent fewer drug cases opened during this 5-year period.

The Department has also recently restructured itself to improve its counterterrorism capabilities. The Department created a National Security Division that brings together the Office of Intelligence and Policy Review (OIPR) and the Counterterrorism and Counterespionage sections formerly part of the Criminal Division. The Department expects this new National Security Division to serve as the principal point of contact with the Office of the Director of National Intelligence (DNI), the Central Intelligence Agency, the Department of Defense, and other components of the intelligence community. Creation of the Department's new National Security Division and the FBI's National Security Branch also implements key recommendations of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission), which recommended greater coordination of intelligence-gathering activities within the Intelligence Community under the DNI.

The Department's new national security elements requires implementing new reporting structures and developing new relationships with other federal, state, and local agencies. Accomplishing these tasks effectively and efficiently presents a critical ongoing challenge for the Department.

Another continuing challenge for the Department, and in particular the FBI, with respect to its counterterrorism effort is to support and integrate to a greater degree non-agent or non-lawyer staff with technical skills. For example, OIG reviews had found that, until recently, the FBI did not adequately value the contributions of its intelligence analysts. Historically, the FBI's general view was that special agents performed the key work of the agency, and intelligence analysts were used primarily as support personnel to assist the agents with their cases. Many special agents appeared not to understand or value the role of intelligence analysts, resulting in poor utilization of analysts. While the FBI is attempting to change this attitude, we believe it still exists in parts of the FBI. We believe the FBI needs to do more to support the work of its intelligence analysts – and other non-agent staff such as scientists and linguists – who are critical to meeting the FBI's changing mission.

As we have discussed in past years, the effectiveness of the FBI – and in particular the FBI's leadership in various areas including counterterrorism – has also suffered because of a lack of continuity due to frequent turnover among all levels of management. For example, the FBI's Counterterrorism Division has had seven leaders in the past 5 years. In addition, the FBI has suffered from rapid turnover in FBI field office managers. This turnover in many key positions has hindered the FBI's ability to transform itself in many areas, including counterterrorism.

In addition, many reviews by the OIG and others have found that the FBI's counterterrorism and intelligence-gathering efforts have been hampered because of difficulties in modernizing its information technology (IT) systems. Although the FBI recently has made progress in improving its management of IT upgrades (which we discuss under the challenge relating to IT systems implementation), agents and

analysts will not benefit from a fully functional case management system for several more years.

The OIG has conducted other reviews of aspects of the Department's activities that relate to its counterterrorism challenges. For example, during the past year we reviewed the FBI's efforts to protect the nation's seaports, the FBI's progress toward achieving biometric interoperability between its fingerprint systems and the system used by the Department of Homeland Security, and the use of Intelligence Research Analysts by United States Attorneys' offices. While each of these reviews found that some positive steps were being taken, each also found problems that illustrate the difficulty the Department faces as it continues to transform itself to better meet the challenge of combating terrorism.

Similarly, a March 2006 OIG audit of the FBI's efforts to protect U.S. seaports from terrorism found that while the FBI has taken steps to enhance its capability to identify, prevent, and respond to terrorist attacks at seaports, important deficiencies remain. We found that the FBI did not always allocate the agents who are responsible for maritime security according to the threat and risk of a terrorist attack on a given seaport. For example, one FBI field office with six significant seaports in its territory had only one Maritime Liaison Agent while another FBI field office with no strategic seaports had five Maritime Liaison Agents. We also noted a lack of coordination between FBI and the Coast Guard that could hinder the two agencies' ability to coordinate an effective response to a terrorist threat or incident in the maritime domain. In addition, the interim Maritime Operational Threat Response (MOTR) plan issued in September 2005 to establish protocols for agencies in responding to terrorist threats in the maritime domain did not resolve issues of overlapping jurisdiction and responsibilities between the FBI and the Coast Guard.

Since we issued our seaports audit, the FBI has informed us that the MOTR has been revised to clarify the roles of the FBI and the Coast Guard in the event of a terrorist attack in the maritime domain or at a seaport. Under the revised protocols, the FBI will be responsible for leading all maritime-related terrorist investigations and for all intelligence collection in the United States. In addition, since issuance of the OIG's report the FBI, Coast Guard, and other MOTR agencies have conducted five national-level joint maritime exercises simulating the new command and control roles established in the new MOTR. These and other actions are important steps towards resolving the coordination issues between the two agencies. However, the FBI still does not assign its agents to protect seaports in a coordinated way, leaving such assignments to the discretion of individual field offices.

In sum, the Department's counterterrorism efforts remain a work in progress. Among the key issues requiring continued attention are allocation of resources based on the threat and risk of terrorist attack; communication and coordination within and among Department components and with other federal, state, and local law enforcement agencies; development of reliable and secure IT systems to facilitate information gathering, sharing, and analysis; human capital planning to provide for hiring, training, and retention of skilled personnel; stability within the management ranks of Department components; and use of the significant investigative and intelligence-gathering tools while respecting civil rights and civil liberties. Many of these issues are discussed in greater detail in the challenges that follow.

2. **Sharing of Law Enforcement and Intelligence Information**: The Department continues to make progress in improving its sharing of law enforcement and intelligence information with federal, state, and local officials. The ability to share such information timely and effectively is critical to the Department's success in preventing acts of terrorism and violent crime. However, ongoing efforts throughout the Department to upgrade IT systems remain a key factor in the Department's ability to more fully meet this challenge.

   Since the September 11 attacks, the FBI has increased the number and frequency of its written and oral communications about terrorism with all levels of the law enforcement and intelligence communities while almost tripling its formal collaborative investigative efforts related to terrorism. For example, in the last 5 years the number of Joint Terrorism Task Forces (JTTFs) has grown from 35 to 101. These multi-agency teams, composed of staff from the FBI, local police and sheriffs' offices, and officials from more than 20 federal law enforcement agencies, investigate terrorism cases within the United States. In addition, members of the Intelligence Community and federal, state, and local participants on the FBI's National Joint Terrorism Task Force – which serves as a liaison for information on threats and leads from FBI Headquarters to the local JTTFs and participating agencies – have access to FBI databases and share access to their organizations' databases in counterterrorism investigations.

   The FBI also has taken action in areas where its initial information-sharing efforts have been deficient. For example, our March 2006 report on the FBI's project to develop its new automated case management system, Sentinel, found that the FBI had not taken adequate steps to ensure that Sentinel would allow sharing of information between the FBI and other intelligence and law enforcement agencies. In addition, we were concerned that Sentinel would not provide a common framework for other agencies' case management systems as initially intended. We recommended that the FBI discuss with other intelligence community and law enforcement agencies their information-sharing requirements to ensure compatibility with those systems in the requirements and design of Sentinel.

   In our current review of the Sentinel project, we found that since the March 2006 audit the FBI has focused more attention on external information sharing needs, coordinating its requirements for Sentinel with the requirements of other Department agencies, the Department of Homeland Security (DHS), and other federal entities, including the Office of the Director of National Intelligence. In addition, Sentinel is being built to meet the standards of the new National Information Exchange Model, a joint Department of Justice/Department of Homeland Security standard that has become the government-wide standard for any new law enforcement and intelligence systems being developed. Adoption of the new standard by other agencies is expected to facilitate government-wide information sharing.

   With respect to sharing other types of important information, the FBI moved forward this past year in sharing fingerprint information with the DHS. The FBI and the former Immigration and Naturalization Service, now part of the DHS, originally developed separate, incompatible automated fingerprint systems in the early 1990s. The FBI's Integrated Automated Fingerprint Identification System (IAFIS) is based on 10 rolled fingerprints, while the DHS's Automated Biometric Identification System (IDENT) system uses 2 flat fingerprints. In May 2005, the agencies resolved the impasse between the differing fingerprint collection requirements that had stalled

interoperability efforts when the DHS agreed to modernize IDENT and convert US-VISIT – its entry/exit and border security system – from a 2- to a 10-fingerprint system.

An OIG report issued in July 2006, the sixth report issued by the OIG on this topic, noted that the FBI and the DHS are in the first phase of a three-phase plan to make IDENT fully interoperable with IAFIS by December 2009. According to the FBI, on September 3, 2006, the FBI and the DHS implemented the first phase of the interoperability plan by deploying a link between the two agencies' systems that will allow the exchange of copies of key immigration and law enforcement data. Yet, despite these improvements, the FBI will continue to face higher than warranted risks that criminal aliens or terrorists will enter the United States undetected until a fully interoperable system is achieved in 2009. To address this challenge, the FBI has taken interim steps to mitigate this risk, which include transmitting "Known or Suspected Terrorists" records to the DHS on a daily basis, improving the availability of IAFIS to other users, and reducing the response time to DHS requests for checks of aliens' fingerprints.

Other aspects of the Department's counterterrorism efforts highlight the need for greater consistency in information sharing. For example, an OIG review examining the use of intelligence research specialists in United States Attorneys' Offices (USAO) to coordinate antiterrorism activities, analyze the relevance and reliability of threat information, investigative leads, and ensure that cases with terrorism connections are identified for prosecution. While we found that individually the specialists made valuable contributions to the USAOs' antiterrorism efforts, we determined that the specialists' overall effectiveness could be increased through improved coordination and guidance. For example, analytical products developed by the specialists were not consistently shared or widely disseminated within the Department. In response to the OIG report, a Department working group is developing standard requirements for analytical work and corresponding quality review of intelligence research products.

The Department's efforts to upgrade and secure information in its IT systems remains a key factor in its ability to more fully meet this information-sharing challenge. The IT and computer security challenges are addressed more fully elsewhere in this document.

In sum, the Department continues to make progress in improving its ability to share more law enforcement and intelligence information both within the Department and with other federal, state, and local law enforcement agencies through improved IT and more effective use of joint task forces. Nevertheless, the Department still faces significant challenges to ensure the timely, effective, and secure sharing of vital intelligence and law enforcement information.

3. **Information Technology Systems Planning, Implementation, and Security**: The Department made important strides this past year in its efforts to upgrade critical IT systems in a timely and cost-effective manner. In the past, widespread and deeply rooted problems, ranging from a lack of critical managerial processes to mismanagement of individual systems, have hobbled attempts by the Department to upgrade some IT systems, particularly the FBI's case management system, and provide employees with the tools needed to maximize their effectiveness.

During the past year, the Department has attempted to more effectively meet this challenge by monitoring the progress of major IT projects through an executive board called the Department Investment Review Board (DIRB). Chaired by the Deputy Attorney General, the DIRB provides high-level oversight as part of the Department's Information Technology Investment Management (ITIM) process. The DIRB's mission is to monitor the Department's major IT investments and ensure they are aligned with the Department's mission.

Improvements in IT management will be sustained only if top Department officials and senior managers in each component maintain a focus on strengthening the general processes associated with IT and the management of mission-critical IT systems.

In the past, the OIG has found that the Department lacked the ability to track the cost of its major IT systems, and more fundamentally exercised little direct control over components' IT projects. Historically, Department components have resisted any form of centralized control over major IT projects, and the Department's Chief Information Office (CIO) does not have direct operational control of component IT management. We believe the Department should consider providing increased control to the CIO for certain high-risk functions and for individual components experiencing difficulty with particular IT systems. These high-risk functions may include hiring for critical positions, completion of system requirements, and oversight of contract administration.

Notwithstanding these concerns, we found that several components made positive strides during the past year to improve their IT management practices. For example, the Drug Enforcement Administration (DEA) has done well in developing its Enterprise Architecture and ITIM processes. Having a mature Enterprise Architecture enables the DEA to make better management decisions on how individual IT projects fit into the agency's overall IT architecture. In addition, well developed ITIM practices better position the DEA to ensure that the development, design, and implementation of its IT projects are performed within cost and schedule baselines.

One of the components that appears to be learning from its past problems is the FBI. Based on a variety of recent reviews, we believe the FBI is making better progress in developing the modern IT systems needed to perform its mission and provide its employees with the ability to effectively analyze, share, and act on the vast amount of information it collects. After a false start with the Virtual Case File (VCF) that cost the FBI 3 years of development time and $170 million, the FBI's effort to replace its antiquated Automated Case Management (ACS) system with a modern case management system is taking shape.

During the past year the FBI instituted better IT investment management processes and controls through its Life Cycle Management Directive. Continuity in the Chief Information Officer position and project management staff – a huge problem in the VCF project – also has stabilized. In addition, the FBI's IT activities have been centralized under the FBI CIO, who now controls IT spending.

With respect to the challenge of successfully implementing the Sentinel project, the FBI's planned $425 million, 45-month project intended to move the FBI away from paper-based records to an electronic case management system, the OIG has found that the FBI is taking important steps to avoid the types of problems that plagued

the VCF project. In particular, the FBI has made significant improvements in its ability to manage a major IT project by establishing ITIM processes, developing a more mature Enterprise Architecture, and establishing a Program Management Office (PMO) dedicated to overseeing the Sentinel project.

In March 2006, the FBI awarded Lockheed Martin Systems a $57 million task order for Phase 1 of Sentinel, with options for an additional $248 million for three additional phases that include the operation and maintenance of the system. Over the next 4 years, Lockheed Martin will be responsible for designing, developing, integrating, testing, deploying, operating, and maintaining Sentinel, which primarily will be based on commercial-off-the-shelf software. Lockheed Martin is performing this work under a cost-plus-award-fee arrangement, similar to the contract used during the Trilogy project. However, we are finding that the FBI is providing much greater control and oversight for Sentinel compared to the weak project management practices evident with Trilogy.

Our preliminary findings in the second Sentinel audit indicate that the FBI has made progress toward resolving most of our initial concerns about planning for the project. However, some concerns, such as the full staffing of the Sentinel PMO, have not yet been fully addressed. Moreover, our current audit has identified additional issues that we believe the FBI must resolve in order to avoid serious problems as the Sentinel project continues through its first phase of development and enters its more challenging and higher-risk second phase in early 2007. These issues include uncertainty over risk mitigation, contingency planning, and total project costs.

In addition to developing and implementing its IT systems in a cost-effective and timely manner, the Department also faces the challenge of convincing Congress that the more than $2 billion it appropriates annually for the Department's IT systems is being spent properly. To assist in this evaluation, in the Department's FY 2006 Appropriations Conference Report Congress directed the OIG to compile 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 March 2006 the OIG completed the first of three planned reports: an unaudited report of the Department's major IT system investments by investment title and component, investment description, implementation status, and actual and projected costs.

The OIG's second report will provide an audited verification of the information detailed in the unaudited report and will discuss the limitations of the Department's financial accounting systems to verify IT system costs. The third OIG report will document existing studies, plans, and evaluations for the Department's major IT systems, comparing these documents to the standards contained in Departmental policy for IT investments. This report also will include an analysis of problems the Department has experienced in the formulation of its IT plans.

Another IT imperative for the Department, made clear in the response to the September 11 terrorist attacks, is the need to develop interoperable IT and communications equipment to aid first responders, law enforcement, and intelligence agencies. To examine the Department's law enforcement communications capabilities, the OIG is auditing a wireless communications system called the Integrated Wireless Network (IWN), a joint project involving the Departments of

Justice, Homeland Security, and Treasury that will support federal law enforcement and homeland security operations throughout the United States.

The Department's current wireless capabilities do not provide law enforcement officers and agents with the support they need because of a 15- to 20-year-old communications systems infrastructure that results in degraded coverage, reliability, and usability. Further, antiquated, stove-piped, land mobile radio systems provide only limited federal-to-federal and federal-to-state and local interoperability. The Department is relying on the proposed IWN project to address these problems. Our report will examine the status of the project and assess whether the Department has accomplished the goals needed to achieve interoperability and cost and spectrum efficiency.

As the Department develops new IT systems, it also must ensure the security of those systems and the information they contain. In addition, the Department must balance the need to share intelligence and law enforcement information with the need to ensure that such information is handled appropriately and that any sharing meets security standards.

Since 2001, the OIG has conducted multiple IT security audits in the Department in response to the Federal Information Security Management Act (formerly the Government Information Security Reform Act). We have noted some improvement in the Department's information security, but we have also continued to identify weaknesses within the Department's management, operational, and technical controls for its sensitive but unclassified and classified systems and deficiencies in the Department's oversight program and related management controls. We found that components were not being held accountable for completing documentation and testing systems, and that stronger monitoring of the Department's certification and accreditation process would have identified and corrected many of the reported system weaknesses. The OIG has recommended that the Department strengthen the roles and responsibilities of the CIO, perform additional testing of systems and security policies, expand the automation of system vulnerability tracking, and conduct additional system security training.

In response to our findings, the Department has made improvements in its oversight of IT security. For example, the CIO and the components are testing the Department's systems more frequently using automated software to track potential system vulnerabilities. In addition, the Department is performing annual IT security awareness training for employees and contractors.

The Department's general controls environment, which represents the structure, policies, and procedures necessary to ensure the secure operation of the Department's information systems, is reviewed during the annual financial statement audits. For FY 2006, a material weakness was issued on the Department's and components' financial systems general and application controls. While the application controls reviews focus primarily on financial management systems, the general controls reviews focus on policies and procedures that apply to all of the Department's information systems. Improvements are still needed in the areas of access controls, system software, application software development and change controls, entity-wide security, segregation of duties, and service continuity. To correct this long-standing material weakness, we believe the Department needs to

improve its monitoring of identified IT weaknesses to ensure that timely corrective actions are performed.

Moreover, several recent incidents in other federal agencies have highlighted vulnerabilities in government safeguards over personal identifying and other sensitive information. Losses of sensitive information at the Departments of Veteran's Affairs and Transportation have highlighted the risk that sensitive data can be compromised if computers or storage media are lost or stolen. Limiting the damage caused by such information losses depends heavily on immediate detection and reporting.

In July 2006, the Office of Management and Budget (OMB) revised the US-CERT reporting procedure to require federal agencies to report all incidents involving personally identifiable information to US-CERT within one hour of discovering the incident. The Department has implemented a reporting system in which equipment losses or data compromises are reported centrally to the DOJ-CERT. Notwithstanding this reporting system, it is not clear what procedures the components follow internally when responding to data breaches or losses. A significant challenge many Department components face is the ability to identify the specific information contained on lost or stolen laptop computers and other IT equipment. Consequently, the OIG recently initiated a review to document the processes and requirements that major Department components follow to report losses of sensitive information, including personal identifying information, the process for tracking personal identifying information contained on electronic media, and the process for notifying affected individuals when personal identifying information is compromised.

In sum, the upgrading of IT systems currently ongoing in several Department components creates major challenges for the Department in securing and safeguarding the sensitive information contained on those systems.

4. **Violent Crime**: As noted above, after the September 11 terrorist attacks, the Department reordered its priorities and elevated preventing future terrorist acts as its top priority. During the ensuing 5 years, the FBI's transformation not only has involved hiring hundreds of new employees, but also shifting agents, analysts, and other resources from traditional criminal investigations to counterterrorism and counterintelligence activities. As a result, as our review assessing the results of the FBI's reallocation of resources found, the Department is investigating and prosecuting significantly fewer traditional criminal matters than it did prior to September 11, 2001.

   During the same period, the Department has allocated less money to state and local governments for crime prevention. For example, the total program funding for the Office of Community Oriented Policing Services (COPS) has decreased from $1.1 billion in FY 2002 to $478 million in FY 2006.

   Yet, the prevention and prosecution of violent crime remains a critical challenge for the Department, particularly when initial indications during this last year suggest that the decline in violent crime may be ending. For example, the latest Uniform Crime Report from the FBI that tracks crime trends across the United States shows a 2.3 percent rise in arrests for violent crime in 2005 compared to the previous year. For 2005, robbery offenses showed the biggest rise, increasing by 3.9 percent compared to the 2004 figure. Aggravated assault increased by 1.8 percent in 2005,

and murder by 3.4 percent. Forcible rape was the only category of violent crime to decline compared to 2004 figures, decreasing by 1.2 percent in 2005.

However, it is important to note that while the 2005 arrest statistics reflect an overall increase in violent crime from the previous year, over a 5-year period the Uniform Crime Report shows a 3.4 percent decrease in violent crime (comparing 2001 rates with 2005 rates) and a 17.6 percent decrease in violent crime over the past 10 years (1996 compared with 2005).

In addition, a second barometer of national crime rates, the National Crime Victimization Survey (NCVS), examines data from a representative sample of 77,200 households on the frequency, characteristics, and consequences of criminal victimization in the United States, specifically rape, sexual assault, robbery, assault, theft, household burglary, and motor vehicle theft. According to Bureau of Justice Statistics NCVS reports, between 2004 and 2005 the number of reported violent victimizations per 1,000 people over age 12 remained nearly constant (21.1 in 2004 and 21.0 in 2005). Specifically, the rate of murder remained at 0.1, rape increased from 0.4 to 0.5, robbery increased from 2.1 to 2.6, aggravated assault remained at 4.3, and simple assault decreased from 14.2 to 13.5.

The Department's challenge with respect to violent crime is to meet its expanded counterterrorism mission while continuing to show leadership in helping reduce violent crime.

In a number of recent reviews, the OIG has examined aspects of the violent crime challenge facing the Department. For example, in a September 2005 report the OIG assessed the impact on state and local law enforcement efforts of the FBI's shift of agents from its criminal program to terrorism and counterintelligence. The OIG found that the FBI opened 28,331 fewer criminal cases in FY 2004 than in FY 2000, a 45-percent reduction. State and local law enforcement officials also told us that their investigative caseloads have increased following the FBI's post-September 11 reprioritization. Many of these officials expressed concern about their agencies' ability to handle the increased workload and commented that the complex crimes that the FBI previously had handled often exceeded their departments' resources, expertise, and jurisdiction.

Several local law enforcement officials noted reduced FBI involvement in violent crimes in their jurisdictions, specifically gang offenses and bank robberies. Some local officials remarked that this reduced effort had created an investigative gap that the local agencies had been unable to completely fill. In contrast, other local representatives said they did not believe the FBI's reduced involvement in these areas had negatively impacted their agencies' operations.

As part of the OIG review, we surveyed state and local law enforcement agencies regarding changes their departments' crime rates between FYs 2000 and 2004. Of the 1,109 respondents to our survey, approximately 50 percent indicated that the overall crime rate in their agencies' jurisdiction had increased during this 5-year period. In particular, 41 percent of respondents said violent crime against persons had increased from FY 2000 to FY 2004; 24 percent said gang-related crimes had increased; and 17 percent cited a rise in bank robberies during this period.

Another indication of the difficulty for the Department in meeting this challenge was highlighted during an August 2006 National Violent Crime Summit in Washington, D.C., convened by the Police Executive Research Forum for mayors and police officials from 45 cities nationwide. During the Summit, several local leaders noted that the shift of federal priorities to terrorism prevention has resulted in less federal funding to combat domestic crime, reductions in police department staffing levels, and more strain on the courts and corrections components of local criminal justice systems.

To address the issue of violent crime, the Department has formed a variety of task forces to focus federal, state and local law enforcement resources on reducing violent crime. These task forces include:

- DEA Mobile Enforcement Teams
- FBI Safe Streets Task Forces
- USMS Regional and District Fugitive Task Forces
- ATF Violent Crime Impact Teams (VCIT)
- Project Safe Neighborhood gun crime task forces
- Weed and Seed task forces to reduce neighborhood violent crime and gang-related activities

In an ongoing review, the OIG is evaluating whether the Department's violent crime task forces are coordinating their investigations to better assist state, local, and tribal law enforcement in reducing violent crime.

A separate OIG review this past year examined ATF's implementation of the VCIT initiative, which currently operates in 20 cities across the country and is slated to expand to 15 more cities by FY 2008. The goal of the VCIT initiative is to decrease the number of homicides and violent crimes committed with firearms in targeted urban areas. The VCIT strategy includes targeting "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 the Department's other law enforcement components.

The OIG evaluation determined that while ATF's VCIT strategy may be an effective tool to reduce violent crime in targeted areas, there was inconsistent application by local VCITs of key elements of the strategy. The OIG also found that ATF's claim in January 2006 that it had met its stated goal was based on insufficient data. In light of the ATF's plans to expand the VCIT program to 15 additional cities in 2007, the challenge for the Department is to consistently implement and evaluate the VCIT strategy in these cities in order to improve the effectiveness of the ATF's efforts to target gun violence in specified urban areas.

In addition, in October 2006 the Attorney General announced the "Initiative for Safer Communities" to target violent crime prevention efforts in selected communities across America that have shown increases in crime. According to the announcement, in the first stage of the Initiative the Department plans to conduct a detailed survey and visit local law enforcement in impacted areas to identify possible factors contributing to the increase in crime. A second phase will focus on policy development by analyzing the findings of the investigative phase to identify the roots of the localized increases in crime. The Initiative's third phase will focus on matching

localized results with established federal programs that are proven to be effective in combating crime and, where necessary, creating new initiatives.

Another challenge that relates to violent crime is the need for the Federal Bureau of Prisons (BOP), as well as state and local corrections facilities, to prepare inmates for life after prison, given that approximately 650,000 people are released from incarceration every year. Studies show that more than half of all offenders were re-arrested within 3 years after release from prison. According to reports from the Bureau of Justice Statistics: "The reentry of serious high-risk offenders into communities across the country has long been the source of violent crime in the United States."

In sum, the Department faces a significant challenge in attempting to reduce violent crime while shifting substantial resources to counterterrorism and counterintelligence activities.

5. **Financial Management and Systems**: The Department has made steady progress during the last several years in addressing several of the major problems identified in the annual financial statement audits, but significant issues remain in financial management systems' general and application controls. In our view the most important challenge for the Department in this area is to implement a unified financial management system to replace the disparate and, in some cases, antiquated financial systems used by Department components.

   One of the key improvements in recent years has been the ongoing and expanded involvement of Department financial managers in assisting components, issuing guidance, and providing greater assistance with component audits and corrective action plans. In addition, the Department has done a better job in recent years meeting expedited due dates for the financial statement audits through detailed planning and revamping of the financial effort.

   For FY 2006, the Department again earned an unqualified opinion and improved sufficiently in the area of financial reporting to reduce its long-standing material weakness on financial reporting to a reportable condition at the consolidated level. The Department components also reduced component material weaknesses from 10 in FY 2005 to 7 this year. In addition, component-level reportable conditions decreased from 8 in FY 2005 to 7 this year. Two components, the Drug Enforcement Administration and Federal Prison Industries, Inc., continued to have no material weaknesses, reportable conditions, or compliance issues.

   Another encouraging result this year was the Department's effective implementation of revised OMB Circular A-123, Appendix A, Internal Control over Financial Reporting. This Circular was recently amended to bring it more in line with the new internal control requirements for publicly traded companies contained in the Sarbanes-Oxley Act of 2002. The Circular requires the Department to document and test its controls in order to provide an annual assessment as to the effectiveness of its internal controls over financial reporting. Under tight time frames the Department was able to prepare its Assessment Methodology and Guide and fully implement this new requirement.

   However, the Department still needs to improve its financial management systems. The material weakness on information system general and application controls still

remains a serious concern in the FY 2006 opinion. In addition, the Department still lacks sufficient automated systems to readily support ongoing accounting operations and financial statement preparation. Inadequate, outdated, and in some cases non-integrated financial management systems do not provide certain automated financial transaction processing activities that are necessary to support management's need for timely and accurate financial information throughout the year. Many tasks still must be performed manually at interim periods and at year-end, requiring extensive manual efforts on the part of financial and audit personnel. These significant, costly, and time-intensive efforts will continue to be necessary for the Department and its components to produce financial statements until automated, integrated processes and systems are implemented that readily produce the necessary information throughout the year.

The Department has placed great reliance on the planned Unified Financial Management System (UFMS) as the fix for many of these automation issues. The UFMS would standardize and integrate financial processes and systems to more efficiently support accounting operations, facilitate preparation of financial statements, and streamline audit processes.

The Department's efforts over the past few years to implement the UFMS to replace the seven major accounting systems currently used throughout the Department have been subject to fits and starts. Currently, none of the Department's accounting systems are integrated with each other. Two years after the Department selected a vendor for the unified system, problems with funding, staff turnover, and other competing priorities have caused delays in implementation of the new system. Consequently, Department-wide accounting information is produced manually, which is costly and undermines the Department's ability to prepare financial statements that are timely and in accordance with generally accepted accounting principles. The DEA is scheduled to begin implementing the UFMS in FY 2008, and current plans are for implementation in all Department components by FY 2012.

To test one aspect of the Department's financial management practices, in April 2005 the OIG issued an audit examining the Department's process for identifying, preventing, and recovering improper and erroneous payments made to vendors by the FBI, BOP, U.S. Marshals Service (USMS), and OJP. We found that some vendor payments and travel reimbursements were not included in one component's risk assessment, while another risk assessment did not identify any specific information about which programs were measured. Also, all components did not have adequate policies and procedures in place to avoid improper payments. In March 2006, at the Department's request the OIG initiated a second audit to evaluate the status of improper payment and recovery auditing activities at the DEA, ATF, Federal Prison Industries, and the Department's Offices, Boards, and Divisions.

In sum, with its positive audit results this year, the Department continues to show improvement in financial management. A major challenge will be to maintain these results while correcting the remaining financial issues. In addition, the Department must address the IT general and application controls issues that remain a material weakness. Complicating these efforts will be the Department's implementation of the UFMS at nine components over the next 7 years, a significant challenge in and of itself.

6. **Detention and Incarceration**: The Department continues to face major challenges in meeting its responsibility to safely, humanely, and economically detain and incarcerate individuals held in the custody of the BOP and the USMS. This challenge is becoming more difficult each year as the number of individuals detained increases dramatically and the cost of confinement rises. In addition to finding the resources to house inmates and detainees, the Department also must provide medical and other services to a population that is aging and often has serious health issues. Moreover, the increasing number of terrorist or high-risk inmates must be closely monitored to prevent further illegal activities. While the Department has made some progress in adapting to these high-risk inmates, more progress is needed.

   The BOP is responsible for approximately 192,000 federal offenders and in FY 2006 received an appropriation of approximately $4.1 billion. In addition, each day the USMS is responsible for housing approximately 54,000 federal detainees (individuals housed primarily in jails under contract with the Department while awaiting trial or sentencing). Within the Department, the Office of the Federal Detention Trustee (OFDT) is responsible for providing oversight of the USMS's detention activities and for managing the budget for housing USMS detainees, which in FY 2006 surpassed $1 billion.

   The BOP's problems in adapting to the challenges presented by high-risk inmates are illustrated by the fact that three convicted terrorists incarcerated at the BOP's highest-security prison for the 1993 World Trade Center bombing had written more than 90 letters to Islamic extremists outside the prison between 2002 and 2004. These extremists included jailed members of a Spanish terror cell with links to other terrorists suspected in the March 2004 attacks on Madrid commuter trains, as well as other Islamic radicals in Spain and Morocco, among them a man charged with recruiting suicide operatives and who used the BOP inmates' letters in his recruitment efforts. A September 2006 review by the OIG examined the BOP's efforts to prevent terrorist and other high-risk inmates from using the mail or the cover of a foreign language to continue or encourage criminal or terrorist activities.

   Our review found that the BOP's monitoring procedures, intelligence analysis, and foreign language capabilities were deficient. We found that the BOP does not adequately read the mail or listen to the telephone calls, visitor communications, or cellblock conversations of terrorist or other high risk inmates. We also found that the BOP does not have sufficient resources to translate inmate communications in foreign languages and lacks staff adequately trained in intelligence analysis techniques to properly assess terrorist communications. Since issuance of the report, the BOP has reported that it is now monitoring 100 percent of terrorist inmates' mail and telephone calls and is translating and screening all correspondence to or from terrorist inmates written in a foreign language.

   Another OIG review in 2004 concluded that due to a shortage of Muslim chaplains, BOP inmates often led Islamic services and were subject only to intermittent supervision from BOP staff members. This practice greatly enhanced the likelihood that radical, inappropriate messages could be delivered to inmates. Since issuance of our report, the BOP has developed enhanced screening criteria for religious services providers. The BOP also accepted the report's recommendations that inmate-led services in all faiths should be reduced, that supervision in the chapel areas should be enhanced, and that reading materials in BOP chapel libraries should be screened more closely. However, the OIG recently learned that the BOP is not screening for

terrorist connections organizations that assist it with recruiting religious services providers. The OIG has recommended to the BOP that it consider vetting these organizations through the FBI in the same way that it screens religious endorsing organizations.

The USMS's efforts to detain individuals held in its custody have also faced significant challenges. Due to the severe shortage of federal detention space, the USMS depends on state and local governments to provide detention space for detainees. As of February 2006, the USMS had entered into more than 1,600 Intergovernmental Agreements (IGAs) under which a state or local government agrees to house federal detainees at an agreed-upon daily rate (a "jail-day rate"). The total budget for USMS detainees is approximately $1 billion per year.

In an ongoing audit, the OIG is examining the IGA process and believes that the Department could realize significant cost savings if it addressed deficiencies in how prices are set in individual IGAs with state and local agencies for detention bed space. In addition, as a result of OIG audits of individual IGAs, we have encouraged the Department to attempt to recover overpayments made to state and local jails. We also have found that the USMS needs to improve its procedures for establishing and monitoring IGAs.

In addition to finding a cost effective way to detain and incarcerate individuals, the Department also must ensure that it is doing so in a safe and humane way. We reported in April 2005 on the shortcomings of federal law in deterring staff sexual abuse at federal prisons. At the time, a correctional officer who engaged in unforced sexual abuse or sexual contact with an inmate was subject only to a misdemeanor offense. We found that federal prosecutors often would not accept these cases because of the low penalties. The OIG report also pointed out a jurisdictional shortcoming in the federal law because it did not apply to federal inmates held in state or local facilities under contract to the federal government rather than in BOP-owned facilities.

Congress corrected those shortcomings during the past year by enacting legislation that elevated the federal crime of unforced sexual abuse or sexual contact by a correctional officer with an inmate from a misdemeanor to a felony offense. In addition, the legislation changed the statute to cover federal inmates housed in contract facilities. While we cannot yet gauge the impact of these statutory changes, we believe that federal prosecutors aggressively using these new tools will make a difference in addressing the serious problem of staff sexual abuse of federal inmates.

OIG agents continue to aggressively investigate allegations that correctional officers have smuggled drugs or contraband into the prison.

The Department faces challenges in keeping drugs out of federal prisons and rehabilitating drug-addicted inmates. In January 2003, the OIG issued a review that found the BOP did not search visitors or monitor visiting rooms adequately, did not search staff or take sufficient measures to prevent drug and other contraband smuggling by BOP staff, and did not provide adequate non-residential drug treatment to inmates.

However, the BOP did not agree with the OIG recommendation to search staff members and their property upon entry to BOP facilities. Since we made the

recommendation, the OIG has continued to investigate cases involving BOP staff smuggling drugs and other contraband, such as cigarettes and cellular phones, into BOP institutions. In many of the cases, staff members admitted that they smuggled drugs and contraband into BOP institutions on several occasions before being caught, and that they carried the drugs into the institutions on their persons or in unsearched property.

The danger of not searching BOP correctional officers was tragically demonstrated on June 21, 2006, when OIG Special Agent William "Buddy" Sentner was shot and killed in the line of duty. Agent Sentner was working as part of an OIG-FBI team to execute arrest warrants on six BOP correctional officers in Florida who had been indicted the previous day on charges of conspiracy to sexually abuse female inmates and introduction of contraband into the correctional facility. During execution of the arrest warrants, one of the correctional officers who was a subject of the warrant opened fire with a personal weapon. Acting with extraordinary courage, Agent Sentner returned fire, killing the correctional officer. Agent Sentner was killed and a BOP Lieutenant was wounded by the correctional officer. We believe that the BOP's recent decision to routinely search staff and their property is a major step in ensuring the security of federal institutions.

7. **Supply and Demand for Drugs**: Controlling the demand for and supply of illegal drugs remains a top management challenge for the Department, as well as for state and local governments throughout the United States. In recent years the Department has made some progress in addressing this challenge, such as the DEA's successful efforts in FY 2005 to dismantle the financial infrastructures of several drug trafficking organizations and recoup nearly $1.4 billion in assets and $477 million in drugs. Despite these and other successes, the challenge to significantly reduce the supply of and demand for drugs remains.

   According to the DEA, seizures of all categories of illegal drugs, except marijuana, increased from FY 2004 to FY 2005. While the DEA has stepped up its efforts to combat methamphetamine, the National Drug Intelligence Center reports that for the second consecutive year more state and local law enforcement agencies nationwide identified methamphetamine as the drug that poses the greatest threat in their area.

   Compounding this challenge is the dramatic increase in the diversion of controlled pharmaceuticals in recent years. According to a 2005 report from the National Center on Addiction and Substance Abuse, the number of people who admitted abusing controlled prescription drugs increased from 7.8 million in 1992 to 15.1 million in 2003, a 94-percent increase. This rate of increase was seven times faster than the increase in the U.S. population for that same period.

   To examine this issue, the OIG completed a follow-up review in July 2006 that assessed 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, such as centralizing its diversion criminal investigations with other criminal investigations, providing additional intelligence resources to diversion investigators, and increasing the number of authorized domestic diversion investigator positions. However, several shortcomings that we identified and reported on in 2002 still exist. 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. In addition, the complicated issue of providing law enforcement authority for its diversion investigators has not been resolved, although the Department is actively pursuing the matter and has forwarded a proposal to OMB. Further, the support that 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.

In addition to addressing the diversion of legal drugs, the Department is confronting the challenge presented by foreign drug trafficking organizations transporting illicit drugs into the United States. An ongoing OIG examination of the DEA's international operations shows that over the last several years the DEA has increased by more than 50 percent the resources dedicated to its foreign offices and international activities – $312 million in FY 2006 compared to $201 million in FY 2000 – a rate significantly higher than that dedicated to domestic drug activities. Our review is also finding that the DEA has maintained good working relationships with the international law enforcement community and is considered vital by foreign officials to effectively combat the world's illicit drug trade. As evidence of its success in this area, the DEA reported that of the 159 organizations identified in FY 2005 as priority targets for its foreign offices, it had disrupted 53 and dismantled 34.

However, we identified several areas in which the DEA could improve its international operations, such as establishing a universal system to catalog and track the investigative leads or requests for assistance received from its foreign offices and ensuring that all foreign law enforcement personnel in special DEA-funded foreign units are appropriately screened to reduce the risk of corruption. Addressing these and other issues identified in the report will enhance the DEA's ability to more effectively combat international organizations that supply the illicit drug market in the United States.

With respect to use of the Internet to illegally distribute drugs, the DEA has developed web education tools to help inform the public that it is illegal to purchase controlled substances over the Internet without a legitimate prescription. In FY 2005, the DEA began working with Internet search engine companies to develop public service announcements that now appear automatically during Internet prescription drug searches. These announcements are designed to alert consumers of the potential dangers and the illegality of purchasing controlled substances, particularly pharmaceuticals, over the Internet.

In addition, the DEA's Demand Reduction Program provides school children with a variety of demand reduction presentations regarding the abuse of controlled prescriptions while its Demand Reduction Office has produced an anti-drug website for teens, www.justthinktwice.com. This site provides information on drug use and drug trafficking, including the health, social, and legal consequences. In addition, many DEA field divisions provide their own demand reduction programs for children, students, parents, teachers, and community leaders.

Since 2003, the DEA has attempted to develop relevant performance measures, most recently through a study funded by the Office of National Drug Control Policy. However, in June 2006 the DEA reported to us that there are no accurate measures of the quantity of drugs available on a national level and it may be impossible to

develop a model that measures the impact of law enforcement activities on drug availability. The DEA stated that it will continue its efforts in this area.

In sum, reducing the supply of illegal drugs, the diversion of legal prescription drugs for improper use, and the demand for illegal drugs remains a critical and ongoing challenge for the Department.

8. **Grant Management**: Since FY 2000, the Department has awarded more than 49,000 grants totaling $23.65 billion to state, local, tribal governments, and other entities. However, we believe that continued shortcomings in the Department's financial and programmatic oversight of grants, coupled with the lack of a mechanism to assess the effectiveness of its varied grant programs, present a continued management challenge for the Department.

   For years OIG audits have identified a variety of management concerns regarding the Department's oversight of grants, such as problems in the grant closeout process, improper uses of grant funds, difficulties in meeting grant objectives, and poor performance measurement of grant effectiveness. These problems persist, and overall we have seen little improvement in how the Department manages its grant programs. The large amount of grant funds awarded annually by the Department coupled with the numerous and decentralized nature of the grantees make this an important management.

   The OIG has performed numerous audits of grant programs managed by OJP, Office on Violence Against Women (OVW), and the Office of Community Oriented Policing Services (COPS) as well as audits of individual grants to state, local, and tribal governments; non-profit organizations; and institutions of higher education. One pervasive theme that has emerged from these reviews is the lack of performance standards, measures, and data to determine what the grants accomplish.

   We have also found that the Department does not exercise its full authority to monitor grants and it has failed to implement simple requirements that could provide greater assurances that the grantees are compliant with grant requirements. For example, the OIG evaluated the FY 2005 announcement and application review process for the Paul Coverdell Forensic Science Improvement Grants (Coverdell Grants) administered by the National Institute of Justice (NIJ), under the legal and fiscal oversight of OJP. NIJ distributed $13.6 million in FY 2005 Coverdell Grants to state and local governments to improve the timeliness and quality of forensic science and medical examiner services and to eliminate backlogs in the analysis of forensic evidence.

   We found that NIJ did not effectively implement a statutory requirement that grant recipients certify that they have a process in place for independent, external investigations if allegations arise of serious negligence or misconduct substantially affecting the integrity of the forensic results. Specifically, we found that NIJ received inadequate certifications because the announcement did not give applicants necessary guidance on what constitutes an independent external investigation and did not require grant recipients to name the entity that would conduct the independent, external investigation.

   We also found management problems when we examined the COPS' administration of the Department grant program to stem the production, distribution, and use of

methamphetamine. Over the past 8 years, Congress has appropriated more than $200 million for grants to state and local law enforcement agencies to combat methamphetamine, currently the most prevalent manufactured drug illegally produced in the United States. We found management weaknesses such as a lack of coordination between officials in the COPS Office, weaknesses in the database that COPS uses to manage and track grants, and insufficient and inconsistent monitoring of grantees. In addition, OIG audits of 44 individual state and local methamphetamine grants totaling more than $56 million identified $9.5 million in questioned costs and numerous accounting and internal control weaknesses.

Similarly, the external audits we conducted in FY 2006 demonstrate a greater need for improved grant oversight by the Department components responsible for administering the grants. For example, we audited a $2.7 million COPS grant to the Pennsylvania State Police intended to pay for police overtime to support community policing and homeland security efforts. The audit found that the Pennsylvania State Police charged for unauthorized fringe benefits, including social security, retirement, hospitalization, health benefits, and regular time salaries, that were outside the scope of the grant. The audit also identified potential program management issues in that the Pennsylvania State Police did not develop performance measures related to activities funded under the grant, nor did it always collect, track, and analyze relevant data to determine specifically what was accomplished with the grant award. In reviewing three other grants totaling approximately $2.8 million awarded by OJP to the North Carolina Department of Crime Control and Public Safety, we determined that unsupported and unallowable costs were reimbursed to the grantee because the grantee did not reconcile the sub-grantees' claims for reimbursement to supporting documentation.

Finally, an effort to improve grant management by creating an Office of Audit, Assessment, and Management (OAAM) within OJP got off to a slow start during the past year. In January 2006, as part of the Department of Justice Reauthorization Act of 2005, Congress gave OJP the authority to create and fund the OAAM, which can help monitor any Department grant. This office could assist OJP by providing more effective oversight of its annual billion-dollar grant programs. However, OJP has been slow to establish or fund this office.

In our view, management of the billions of dollars in Department grants is in need of significant improvement and is a critical Department challenge.

9. **Civil Rights and Civil Liberties**: The Department faces the challenge of aggressively pursuing its counterterrorism and law enforcement missions while at the same time safeguarding civil rights and civil liberties. FBI Director Mueller crystallized the importance of this challenge in a recent speech when he noted: "As we recognize the necessity of intelligence gathering, we must also recognize the need to protect our civil rights. It has always been my belief, that in the end, we will be judged not only on whether we win the war against terrorism, but also on how we protect the civil rights we cherish."

   One positive step during this past year was the Department's creation of the Office of Privacy and Civil Liberties within the Office of the Deputy Attorney General. This office is responsible for privacy policy and for developing appropriate civil rights safeguards, particularly related to counterterrorism issues. In February 2006, the Department appointed a Chief Privacy and Civil Liberties Officer and two months

later initiated the Privacy and Civil Liberties Board, composed of senior representatives from major Department components. The Board's mission is to (1) examine the activities of the Department to ensure that it continues to fully protect the privacy and civil liberties of all Americans; (2) recommend policies, guidelines, and other administrative actions; and (3) refer credible information pertaining to possible privacy or civil liberties violations to the appropriate office for prompt investigation. A challenge for the Department is to integrate this new Office of Privacy and Civil Liberties in the work of the Department so that office can play a meaningful role in the development and implementation of Department policy that may affect civil rights and civil liberties issues.

The OIG continues to play an important role in reviewing Department programs that either directly or indirectly impact civil rights and civil liberties issues. Examples of such recent OIG reviews include our examination of reports of possible intelligence violations forwarded to the President's Intelligence Oversight Board and our review of the FBI's interviews of protesters connected to the 2004 Democratic and Republican National conventions. Currently, we are conducting reviews relating to other civil rights issues, including the FBI's use of National Security Letters and subpoenas for records under Section 215 of the Patriot Act. In addition, we have continued to monitor actions that the Department has taken to resolve issues that we highlighted in previous reviews.

For example, in June 2003 the OIG issued a review that examined the treatment of aliens held on immigration charges in connection with the investigation of the September 11 attacks. We made several findings about the civil rights and civil liberties of the detainees, including that the FBI made insufficient efforts to distinguish between aliens who were subjects of the FBI terrorism investigation and those who were encountered coincidentally to the investigation, the Department and the FBI's policy and procedures for handling the detainees led to the detainees remaining in custody much longer than necessary, the conditions under which the detainees were detained at the Metropolitan Detention Center in Brooklyn, New York, were unduly harsh, and some MDC correctional officers engaged in a pattern of physical and verbal abuse against the detainees.

We made a series of recommendations related to the FBI, the BOP, and leadership offices at the DOJ, as well as immigration issues now under the jurisdiction of the DHS. All but one of the recommendations have been resolved. The one open recommendation calls for the Department and the DHS to enter into a memorandum of understanding (MOU) to formalize policies, responsibilities, and procedures for managing a national emergency that involves alien detainees. While the Department and DHS agreed with this recommendation and began negotiating over language in the MOU to implement the recommendation, the MOU still has not been finalized.

Consistent with Section 1001 of the USA PATRIOT Act, the OIG released to Congress its eighth semiannual report in March 2006 and ninth semiannual report in August 2006 describing the OIG's activities related to civil rights and civil liberties complaints. Both reports summarize investigations and reviews undertaken by the OIG in furtherance of its Section 1001 responsibilities. In addition, 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 possible violations reported by the FBI

to the IOB in FY 2004 and 2005 and the process used by the FBI to report such violations.

Examples of the possible 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 Foreign Intelligence Surveillance Act (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 an FBI National Security Letter. However, not all 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 reported matters in both years we examined. We intend to continue to review these potential IOB violations and report on our findings in future reports.

In some of our reviews, we concluded that Department employees had not committed civil rights or civil liberties violations as was alleged. For example, in April 2006 the OIG issued a report on the FBI's use of its investigative authorities to conduct interviews of potential protesters in advance of the 2004 Democratic and Republican national political conventions. The OIG initiated this investigation after reports that dozens of people had been interviewed in at least six states, including anti-war demonstrators and political demonstrators and their friends and family members. The OIG review did not substantiate allegations that the FBI improperly targeted protesters for interviews in an effort to chill the exercise of their First Amendment rights at the conventions. The report concluded that the FBI's interviews of potential convention protesters and other related interviews, together with the FBI's related investigative activities, were conducted for legitimate law enforcement purposes and were based upon a variety of information related to possible bomb threats and other violent criminal activities.

The OIG recently initiated a review to examine allegations that the FBI targeted domestic advocacy groups for scrutiny based solely upon their exercise of rights guaranteed under the First Amendment of the United States Constitution. The review is examining allegations regarding the FBI's investigation, and the predication for any such investigation, of certain domestic advocacy groups, including the Thomas Merton Center, Greenpeace, and People for the Ethical Treatment of Animals.

We also continue to investigate individual allegations of violations of civil rights and civil liberties and refer our findings to the appropriate agency for action. For example, the OIG examined allegations raised by an Egyptian national concerning alleged improper treatment during his arrest by the FBI on September 12, 2001, and his incarceration in a federal prison. While the investigation did not substantiate the allegation that BOP employees physically abused the inmate during his incarceration, we did find that the inmate was subjected to body cavity searches that did not comply with BOP policy. We also found that the correctional officers later provided false statements and tried to conceal their role in this incident and that BOP staff failed to properly maintain and safeguard videotapes of this inmate during his detention. While the U.S. Attorney's Office declined prosecution, the OIG provided its report of investigation to the BOP for appropriate administrative action against the correctional officers.

The Department's increased efforts to collect and share information with its law enforcement and intelligence partners also presents a significant challenge to the

Department's efforts to protect civil rights and civil liberties. For example, information-sharing imperatives contained in various Attorney General Guidelines, Presidential Decision Directives, and recommendations from study groups like the WMD Commission underscore the challenge of reconciling the Department's need for effective intelligence tools with the need to observe existing legal, operational, and administrative constraints on these potentially intrusive authorities.

Likewise, investigative and intelligence authorities enacted or expanded in the Patriot Act and the Patriot Improvement and Reauthorization Act of 2005 invest broad new information-gathering powers in FBI agents and their supervisors, often permitting these tools to be approved at the field office level on a minimal evidentiary predicate. For example, when Congress lowered the evidentiary threshold for issuing National Security Letters in the Patriot Act through amendments to pre-existing statutes, it authorized the FBI to collect information such as telephone records, Internet usage, and credit and banking information on persons who are not subjects of FBI investigations. This means that the FBI – and other law enforcement or Intelligence Community agencies with access to FBI databases – is able to review and store information about American citizens and others in the United States who are not subjects of FBI foreign counterintelligence investigations and about whom the FBI has no individualized suspicion of illegal activity.

Consequently, the Department and the FBI in particular need to be mindful of the potential for any abuse of these authorities and the need for aggressive oversight by first-line supervisors, field office and headquarters managers, legal counsel, and established internal and external oversight mechanisms.

In sum, as Director Mueller pointed out, the Department needs to protect civil rights and civil liberties while pursuing its important counterterrorism and crime fighting missions. How the Department balances these issues is one of its most important challenges.

10. **Cybercrime**: Cybercrime is a broad area that ranges from on-line sexual predators to theft of intellectual property to computer intrusions known as "hacking." With rapid technological advances and the widespread use of the Internet, cybercrime is a growing source of criminal activity and an emerging challenge for the Department and law enforcement nationwide.

    The Internet Crime Complaint Center, which is jointly operated by the FBI and a congressionally funded, non-profit corporation called the National White Collar Crime Center, received 231,493 complaints in 2005, an 11.6 percent increase over the previous year. In addition, according to a national survey conducted this year by University of New Hampshire researchers and cited by the Attorney General at a recent conference addressing cybercrimes against children, one third of all children aged 10 to 17 who used the Internet were exposed to unwanted sexual material.

    The FBI's efforts to address cybercrime were fragmented among many different units until 2002. At that time the FBI – recognizing the international aspects and national economic implications of cyber threats – created a Cyber Division at FBI headquarters to manage and direct this developing program. In March 2003, the FBI issued the Cyber Division National Strategy to provide a strategic and coordinated approach to the cybercrime threat. The strategy outlines four objectives: identifying and neutralizing individuals or groups conducting computer intrusions and spreading

malicious code; intellectual property thieves; internet fraud; and on-line predators that sexually exploit or endanger children.

In the Department, the Criminal Division's efforts to fight cybercrime are centered in the Child Exploitation and Obscenity Section, which coordinates efforts to prosecute Internet sex crimes against children, and in the Computer Crime and Intellectual Property Section (CCIPS), which focuses on electronic penetrations, data thefts, and cyberattacks on critical information systems. In response to the growing threat of cybercrime, CCIPS has nearly doubled in size over the past 6 years, to 35 attorneys. These attorneys prosecute cases as well as provide assistance to other law enforcement officials and Assistant United States Attorneys pursuing cybercrime cases.

In addition, the Department has developed other initiatives to fight cybercrime. For example, in March 2004 the Department established a Task Force on Intellectual Property that includes within its focus computer crimes involving theft of intellectual property. The Department also has greatly expanded the Computer Hacking and Intellectual Property "CHIP" Program at the United States Attorneys' Offices, which is designed to increase the number of prosecutions of these types of cases and to improve coordination of these cases with other Department components. As of June 2006, more than 230 attorneys throughout the country have been assigned to the CHIP program.

In May 2006, the Department announced Project Safe Childhood, a new program designed to protect children from sexual abuse and exploitation on the Internet. The project, led by the 94 United States Attorneys, will develop regional task forces to investigate and prosecute crimes against children facilitated through the Internet or other electronic media and communications devices. The project is intended to integrate federal, state, and local efforts; increase the number of cases prosecuted in federal court where stiffer punishment is available; provide training to federal, state, and local law enforcement partners in order to more effectively investigate and prosecute these cases; and increase community awareness of this problem in order to provide the tools to parents and children seeking to report possible violations.

These new programs, while a positive step in the efforts to combat cybercrime, nevertheless present significant implementation challenges for the Department. As part of the OIG's review of the DEA's efforts to control pharmaceutical diversion, we examined a series of actions the DEA has taken to control the increasing use of the Internet to obtain controlled pharmaceuticals. Since the late 1990s, hundreds of Internet pharmacies have been established through which large amounts of pharmaceuticals can be easily purchased with a credit card and without a prescription. According to an estimate in the July 2005 study by the National Center on Addiction and Substance Abuse, entitled Under the Counter: The Diversion and Abuse of Controlled Prescription Drugs in the U.S., the number of Internet pharmacies in operation reached as many as 1,400. Other reports found that 17.4 million people visited online pharmacies in the fourth quarter of 2004, an increase of 14 percent from the previous quarter.

In our review of the DEA's efforts in this area, we found that from FY 2002 to FY 2005 the DEA increased the percentage of time that its diversion investigators spent investigating Internet diversion cases from 3 percent in FY 2002 to 11 percent FY 2005. The DEA also developed an Internet strategy and established telephone and

web-based hotlines for the public to report suspicious Internet pharmacies. However, we found that most diversion investigators had not received the specialized training they needed to conduct successful Internet investigations and that most diversion investigators lacked the undercover equipment they needed to conduct Internet investigations.

In sum, addressing the varied facets of cybercrime presents a series of challenges for the Department. While the Department has developed several initiatives to combat aspects of this complicated crime, the Department must continue to build upon these initiatives to respond to this growing challenge.