OIG Top Management and Performance Challenges in the Department of Justice

MEMORANDUM FOR THE ACTING ATTORNEY GENERAL
THE ACTING DEPUTY ATTORNEY GENERAL

FROM: GLENN A. FINE
INSPECTOR GENERAL

SUBJECT: Top Management and Performance Challenges in the Department of Justice – 2007

Attached to this memorandum is the Office of the Inspector General's (OIG) 2007 list of top management and performance challenges facing the Department of Justice (Department). We have prepared similar lists since 1998, initially in response to Congressional requests. By statute, this list is now required to be included in the Department's annual Performance and Accountability Report.

As in past years, the challenges are not presented in order of priority – we believe that all are critical issues facing the Department. However, it is clear that the top challenge facing the Department continues to be its ongoing response to the threat of terrorism. Several other top challenges are closely related to and impact directly on the Department's counterterrorism efforts.

This year we have added to the list the challenge of restoring confidence in the Department and its operations. The Department has faced significant criticism of its actions and endured a great deal of turmoil during the past several months. We believe that this situation, coupled with numerous vacancies in senior positions, creates a challenge for the new Attorney General and the Department's leaders to reestablish public confidence in the Department.

We hope that this document assists Department managers in developing strategies to address the top management and performance challenges facing the Department. We look forward to continuing to work with the Department to address these important issues.

Attachment

1. Counterterrorism: A critical challenge facing the Department of Justice (Department) is its ongoing effort to detect and disrupt acts of terrorism. Six years after adopting counterterrorism as its highest priority, the Department continues to enhance its counterterrorism capabilities, but this challenge requires continual attention and improvement.

To assist in this process, the Office of the Inspector General (OIG) continues to review Department activities that relate to its counterterrorism challenge. While these reviews are finding that the Department in general and the Federal Bureau of Investigation (FBI) in particular are taking a series of positive steps, our reviews are also finding problems that illustrate the challenges the Department and the FBI face.

The FBI continues its transformation into a more proactive, intelligence-driven agency. One issue that we believe affects the FBI's efforts in making this transition is the frequent rotations and turnover within its senior management ranks. Understanding the organization, leadership, linkages, operational methodologies, strategies, and philosophies of various terrorist organizations, as well as forging relationships within the intelligence community, takes time to develop. As a result, frequent turnover in key positions can have detrimental consequences if not managed carefully.

The OIG continues to examine a variety of FBI programs that directly affect its counterterrorism mission. For example, since the September 11 attacks the FBI has led the effort to create the Terrorist Screening Center (TSC), a multi-agency organization created to consolidate information on domestic and international terrorists and provide 24-hour, 7-day-a-week responses for screening individuals against the consolidated terrorist watchlist. Prior to establishment of the TSC, the federal government relied on more than a dozen separate watchlists 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, or are stopped by a local law enforcement officer for a traffic violation.

A June 2005 OIG report found that the TSC had made significant strides in becoming the government's single point-of-contact for law enforcement authorities requesting assistance in identifying individuals with possible ties to terrorism by developing a consolidated terrorist watchlist database. However, our review found that the TSC had not ensured that the information in that database was complete and accurate. For example, we found instances where the consolidated database did not contain names that should have been included on the watchlist.

In September 2007, the OIG issued a follow-up audit which found that the TSC had enhanced its efforts to ensure the quality of terrorist watchlist data, had increased staff assigned to data quality management, and had developed a process and a separate office to address complaints filed by persons believing they were inaccurately included on the watchlist. However, our audit also found that the TSC's management of the watchlist continues to have weaknesses. For example, the TSC still relies on two versions of the watchlist database, and we identified several known or suspected terrorists who were not watchlisted appropriately. We also concluded that the TSC needs to further improve the accuracy of watchlist records. Although the TSC had increased its quality assurance efforts since our last review, it continues to lack important safeguards for ensuring data integrity.

In another area affecting the FBI's counterterrorism efforts, we found that the FBI has made progress in improving its hiring, training, utilization, and retention of intelligence analysts, although in some areas the progress had been slow and uneven. On the positive side, the FBI is using threat and risk-based criteria to determine the number of analysts needed, establishing hiring goals based on the projected need for additional analysts, assessing which tasks could be more efficiently performed by other support personnel, and developing succession and retention plans for analysts. However, improvement is needed in the time required to hire analysts. In addition, the FBI has struggled to design a satisfactory training program for its counterterrorism agents and analysts, and we found that many special agents still do not fully understand or appreciate the role of analysts.

A significant number of OIG reviews have found that the FBI's counterterrorism and intelligence-gathering efforts have been hampered because of outdated information technology (IT) systems. The FBI recently has made progress in improving its management of its IT upgrades (which we discuss under the challenge relating to IT systems implementation), but the FBI will not benefit from a fully functional case management system for at least two more years.

A critical part of this overall challenge is to ensure that the FBI pursues its counterterrorism responsibilities while adequately protecting civil liberties. A March 2007 OIG review identified serious failures of accountability in the FBI's misuse of national security letter (NSL) authorities (discussed in greater detail under the challenge related to civil rights and civil liberties). This OIG report found that the FBI did not provide adequate guidance, controls, or training on the use of sensitive NSL authorities, and the FBI's oversight of NSLs was inconsistent and insufficient.

To achieve success in its counterterrorism efforts while respecting civil liberties, the Department must maintain a strong focus on ensuring accountability in its activities. One important step the Department took this past year in the aftermath of the OIG's NSL report was assigning the National Security Division (NSD) oversight of various intelligence-related activities. The NSD also recently announced a reorganization that creates an "Office of Intelligence" to replace the Office of Intelligence Policy and Review. The NSD's challenge moving forward is to help instill throughout the Department a commitment to both effectiveness and accountability in all counterterrorism-related and intelligence-gathering operations.

The Department also must maintain accurate statistics measuring its counterterrorism activities. Congress and Department managers use terrorism-related statistics, for example, to make funding and operational decisions. In February 2007, we completed an audit of the Department's internal controls over terrorism reporting that examined whether Executive Office for U.S. Attorneys (EOUSA), Criminal Division, and FBI terrorism-related statistics were accurate.

Our audit found that 20 of the 26 statistics the OIG tested were significantly overstated or understated. The Department reported inaccurate statistics for a variety of reasons, including that Department components could not provide support for the numbers reported, could not provide support for a terrorism link used to classify statistics as terrorism-related, and could not document that the activity reported occurred in the period reported. The Department's collection and reporting of terrorism-related statistics was decentralized and haphazard. For many of the statistics, Department officials either had not established internal controls to ensure the statistics were accurately gathered, classified, and reported or did not document the internal controls used. In response to the audit, EOUSA, the Criminal Division, and the FBI agreed to implement internal controls to ensure that terrorism-related statistics are reported accurately in the future.

Compared with several years ago, we have seen substantially more involvement among various Department components in counterterrorism efforts and information sharing on counterterrorism issues. For example, in late 2006 the Federal Bureau of Prisons (BOP) created a Counterterrorism Unit to assist in the monitoring of federal prisoners believed to have links to terrorist organizations or activities. In addition, the Drug Enforcement Administration's (DEA) Office of National Security Intelligence shares information with the Intelligence Community to identify and disrupt illegal drug trafficking and corresponding ties to counterterrorism operations. We are currently auditing the effectiveness of intelligence reports and related products produced by DEA's Intelligence Research Specialists and Reports Officers, and DEA's efforts to recruit, train, and utilize these specialists.

In sum, the Department's counterterrorism efforts remain a work in progress. While the Department continues to improve its counterterrorism efforts, it still faces significant management challenges in this area.

2. Restoring Confidence in the Department of Justice: An immediate challenge facing Department of Justice leadership is the need to restore confidence in the Department and its operations, both with Department employees and with the public. Recently, the Department has faced significant criticism of its actions and ongoing congressional and internal investigations on a variety of topics, including the removal of U.S. Attorneys and allegations of improper hiring practices for career attorney positions at the Department. These and other allegations regarding the integrity and independence of the Department have affected the morale of Department employees and public confidence in the decisions of Department leaders. This turmoil, combined with numerous high-level vacancies, creates an urgent challenge for the Department's leaders to reestablish public confidence in the independence and integrity of the Department.

In addition, recent resignations by the Attorney General, the Deputy Attorney General, and the Associate Attorney General leave the Department without any of its three most senior Senate-confirmed leaders for the first time in memory. As of October 1, 2007, only 3 of the Department's 11 presidentially appointed Assistant Attorney General positions were filled by Senate-confirmed appointees. Further, 23 of the 93 U.S. Attorney positions were occupied by interim or acting U.S. Attorneys. Vacancies in many key leadership positions have resulted in delayed decision-making or lack of decision-making on a variety of important issues.

The immediate challenge for the incoming Attorney General and his team is to restore confidence in the integrity and independence of the Department – with Department employees, with Congress, and with the public. Accomplishing this rebuilding of trust, while at the same time managing the Department's day-to-day operations, is a critical challenge for the Department and its new leadership.

3. Financial Management and Systems: The Department has continued to make progress in addressing several of the major problems identified in the OIG's annual financial statement audits. However, the Department still lacks sufficient automated systems to readily support ongoing accounting operations and preparation of financial statements. As discussed in past years, the most important challenge facing the Department in this area is to successfully implement an integrated financial management system to replace the disparate and, in some cases, antiquated financial systems used by Department components.

For fiscal year (FY) 2007, the Department again earned an unqualified opinion and improved its financial reporting. This year, at the consolidated level, the Department had two significant deficiencies compared to one material weakness and one reportable condition for FY 2006. It improved sufficiently in the area of information systems general and application controls to reduce its long-standing "material weakness" to a "significant deficiency." The Department's other significant deficiency related to financial reporting in various components. In addition, Department components reduced component material weaknesses from seven in FY 2006 to four in FY 2007. However, once again much of this success was achieved through heavy reliance on contractor assistance, and we remain concerned about the sustainability of these ad hoc and costly efforts in future years.

In recent years, a key improvement in the Department's financial statement audits has been the expanded involvement of Department managers in issuing guidance and providing greater assistance with component audits and corrective action plans. In FY 2006, the Department successfully implemented the revised Office of Management and Budget (OMB) Circular A-123, Appendix A, Internal Control over Financial Reporting. This Circular was amended to more closely align with the new internal control requirements for publicly traded companies contained in the Sarbanes-Oxley Act of 2002. The revised Circular requires the Department to document and test its internal controls in order to provide an annual assessment as to the effectiveness of those internal controls over financial reporting.

The Department expanded its OMB Circular A-123 internal control review process in FY 2007 to include assessments of the components' information systems control environment and improper payment improvement program. These actions have enabled the Department to monitor the components' corrective action plans more timely and, when necessary, provide additional resources to correct control weaknesses.

Yet, currently none of the Department's seven major accounting systems are integrated with each other. In some cases the components' inadequate and outdated financial management systems are not integrated with all of their own subsidiary systems and therefore do not provide automated financial transaction processing activities 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. These costly and time-intensive efforts will continue to be necessary to produce financial statements until automated, integrated processes and systems are implemented that readily produce the necessary financial 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 is intended to standardize and integrate financial processes and systems to more efficiently support accounting operations, facilitate preparation of financial statements, and streamline audit processes. It also will enable the Department to exercise real-time centralized financial management oversight while maintaining decentralized financial management execution.

However, 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. Three years after the Department selected a vendor for the unified system it has made little progress in deploying the UFMS. The Department notes that problems with funding, staff turnover, and other competing priorities have caused the delays in implementing the UFMS. We reported last year that the DEA was scheduled to be the first component to fully implement UFMS in FY 2008, but now it is projected to begin implementation in FY 2009. Additionally, implementation of the UFMS is not scheduled to be completed in all components until FY 2012. Until that time, Department-wide accounting information will have to continue to be produced manually, a costly process that undermines the Department's ability to prepare financial statements that are timely and in accordance with generally accepted accounting principles. Furthermore, the FBI and USMS will not be able to achieve compliance with the Federal Financial Management Improvement Act of 1996 requirement to record all activity at the United States Standard General Ledger transaction level until the UFMS has been fully implemented.

In sum, the Department continues to show improvement in its overall financial management, with another year of positive audit results and successful implementation of OMB Circular A-123. The biggest challenges facing the Department are to make additional progress on its outstanding financial management and information systems general and application controls issues while moving forward on implementing the UFMS throughout the Department.

4. Grant Management: Grant management is a continuing top challenge, with the Department awarding approximately $3 billion in grants in FY 2007 and approximately $23 billion in the previous 7 years. Yet, the Department components that award grants still lack adequate financial and programmatic oversight of their varied grant programs, and they have yet to develop consistent mechanisms to assess the effectiveness of their grant programs, raising questions about how effectively these grant funds are being spent.

This year OIG audits continue to identify a variety of management concerns regarding the Department's oversight of its grant programs, including problems in the grant closeout process, improper use of grant funds, difficulties in meeting grant objectives, and poor performance measurement of grant effectiveness. These are well known problems, but over the years we have not seen significant improvement in how the Department manages these programs.

While it is important to efficiently award the billions of dollars in grant funds appropriated by Congress annually, it is equally important that the Department maintains proper oversight over the grantees' use of these funds to ensure accountability and to ensure that these funds are effectively used as intended. Too often the OIG has observed a misplaced emphasis on expeditiously awarding grants and a lack of a commensurate emphasis on monitoring the grants awarded.

For example, during 2007 our audit of the Department's overall grant closeout process identified significant concerns over grant management activities. In particular we found that the Office of Community Oriented Policing Services (COPS), the Office of Justice Programs (OJP), and the Office of Violence Against Women (OVW) failed to ensure that grants were closed in a timely manner. We found that only 13 percent of grants were closed within 6 months after the grant end date as required by federal regulation and agency policy. Our audit also identified over 12,000 expired grants more than 6 months past the grant end date that had not been closed. Of these grants, 67 percent had been expired for more than 2 years. We recommended that the Department improve the timeliness of grant closeouts, drawdowns on expired grants, and management of unused grant funds on expired grants.

Since issuance of our report, the Department had closed more than 9,000 expired grants. In particular, the COPS Office has worked hard during the past year to improve its grant closeout process by seeking to ensure that expired grants are closed within 6 months of the grant end date, COPS grantees are prohibited from drawing down grant funds after the end of the 90-day liquidation period unless an extension is requested by the grantee, and any unused grant funds for expired and closed COPS grants are deobligated within 6 months after the grant end date. However, OJP and OVW still need to implement procedures to ensure that grants are closed within 6 months after the grant end date and that grantees are prohibited from drawing down grant funds after the end of the 90-day liquidation period unless an extension is requested by the grantee and approved by the awarding agency.

An ongoing OIG audit of OJP's Human Trafficking grant program, a program which is intended to assist human trafficking victims and funds task forces to identify and rescue victims, is also finding problems with improper use of grant funds, the design and management of the program, and poor performance measures to assess the program's effectiveness.

Another ongoing audit is reviewing the Southwest Border Prosecution Initiative (SWBPI), an OJP administered program that reimburses state and local governments for costs associated with the prosecution and detention of criminal cases declined by the U.S. Attorneys' Offices. Preliminary findings in this audit also indicate weaknesses in monitoring and oversight of grant funds.

Other OIG external audits in FY 2007 demonstrated a continuing need for improved grant oversight by the Department components responsible for administering grants. For example, in a $3 million COPS grant awarded to the City of Philadelphia Police Department to pay for overtime and homeland security efforts, we questioned over $1.2 million in overtime costs and found material weaknesses in several essential grant conditions. Our reviews of other grants showed similar weaknesses, including poor budget management and control. Overall, our external audits find that the Department's administration of grant programs needs to be strengthened through better monitoring and by obtaining more timely and definitive information about project funding and the progress of program implementation.

Unfortunately, during this past year OJP has made little progress in staffing its new Office of Audit, Assessment, and Management (OAAM). Created by Congress, this office was intended to improve internal controls and streamline and standardize grant management policies and procedures across OJP. Yet, as of September 2007 OJP had not hired a director for OAAM because OJP said it was awaiting a Senior Executive Service position. OAAM is comprised of three divisions, each managed by a deputy director. Only one OAMM division, the Audit and Review Division, is close to fully staffed. Eleven of the Division's 18 planned positions are filled, 1 is vacant, 2 positions are filled pending security clearances, and 4 positions are scheduled to be filled in October 2007 by transferring employees from other OJP divisions. The Program Assessment Division, staffed by a deputy director and three program assessment analysts, has 10 vacancies. OJP has not staffed any of the four positions in the Grants Management Division. Our assessment is that OJP has devoted insufficient effort to ensuring that this office oversees and monitors grants, despite the importance of this mission.

In April 2007, Congress approved a revised organizational structure for OJP. Earlier in 2007 OJP reported that it had implemented several modifications to its grants management practices and systems, including: (1) enhanced the web-based Grant Management System, including implementing a closeout module to improve the timeliness of the grant closeout process; (2) a standard grant monitoring tool that contains programmatic, financial, and administrative components; and (3) an OJP-wide grant assessment tool that utilizes 15 criteria to determine grantees in need of assistance through on-site monitoring. Future OIG audits will assess whether this new structure will help OJP correct longstanding deficiencies in its oversight of its annual multi-billion-dollar grant programs.

This past year, the Department also established the National Procurement Fraud Task Force (NPFTF), which seeks to prevent, detect, and prosecute procurement and grant fraud. As part of that effort, the OIG is chairing the Grant Fraud Committee of the task force. To put the importance of grant issues in perspective, in FY 2005 grant expenditures throughout the federal government totaled more than $440 billion, exceeding the $385 billion spent during the same period on federal contract actions.

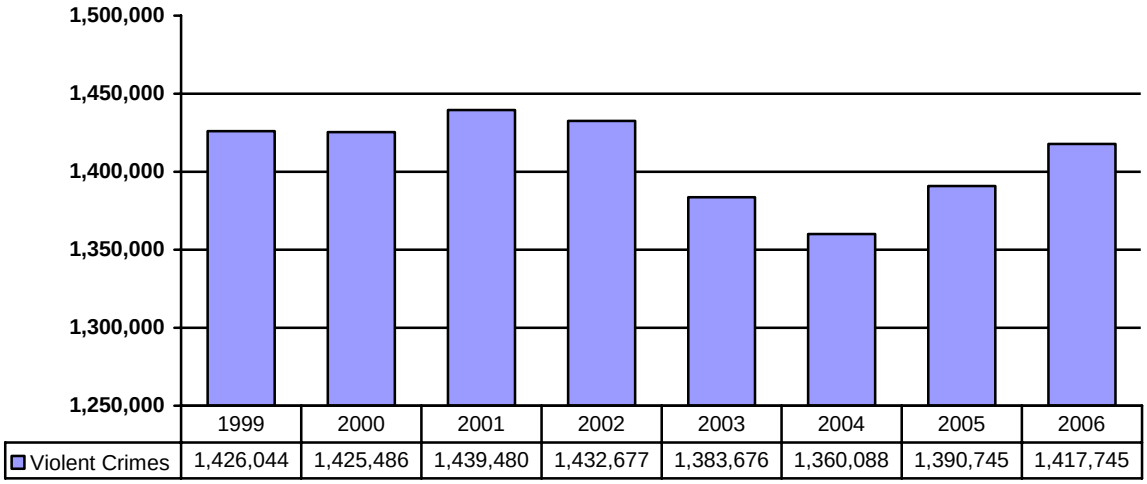
The NPFTF Grant Fraud Committee is focusing on three areas to help improve the ability of the federal government to prevent, detect, investigate, and prosecute grant fraud: (1) examining ways to enhance information sharing concerning cases and issues related to grant fraud; (2) coordinating efforts to provide training to auditors, agents, and prosecutors on detecting, investigating, and prosecuting grant fraud; and (3) conducting outreach to agency program managers who manage federal grant programs and grantees to coordinate prevention, detection, and investigation of grant fraud and to communicate best practices in these areas.

As part of the initiative, the OIG has analyzed past audit reports and investigations to create a common list of grant fraud indicators. In addition, we have developed an internal control survey to quickly assess the risk of fraud related to grantee operations. We believe that these initiatives can help the Department identify controls to reduce the opportunity for grant fraud and mismanagement to occur.

5. Violent Crime: The Department of Justice's recently issued Strategic Plan recognizes as two of the Department's top priorities the need to "reduce the threat, incidence and prevalence of violent crime" and to "strengthen partnerships for safer communities and enhance the Nation's capacity to prevent, solve, and control crime." Achieving sustained progress toward these goals continues to present a significant management challenge for the Department, particularly in light of a second year of increases at the national level in violent crimes reported to law enforcement and the shift of the Department's top priority to preventing terrorism.

National statistics on the number and rate of violent crime for 2005 and 2006 suggest that the decline that began in the 1990s is ending. For example, as Chart 1 shows, the FBI Uniform Crime Report on trends in the number of violent crimes reported to law enforcement across the United States shows a 2.3-percent increase in violent crime in 2005 over 2004 and a 1.3 percent increase in violent crime in 2006 over 2005. For 2006, robbery showed the biggest rise, increasing by 6 percent compared to 2005 figures and murder increased by 0.3 percent. In contrast, the 2006 figures show decreases in two categories: forcible rape declined by 1.9 percent and aggravated assault declined by 0.7 percent.

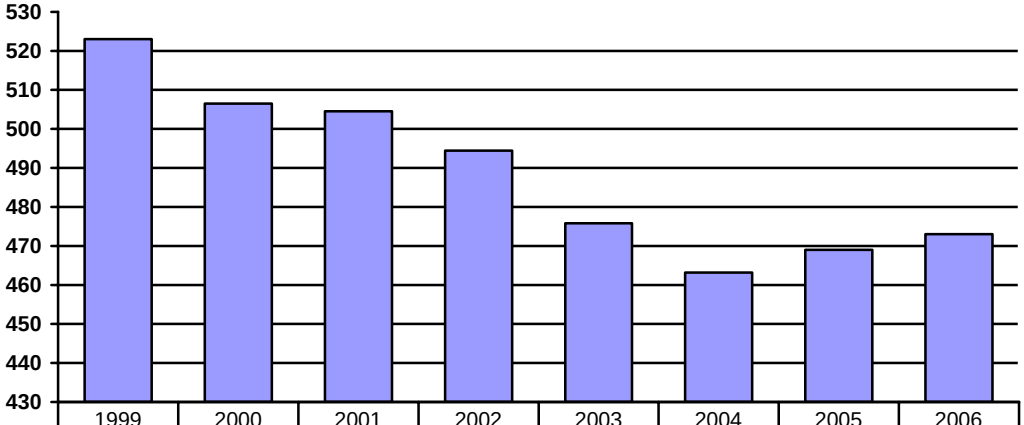
Chart 1 - Number of Reported Violent Crimes, 1999 - 2006



	1999	2000	2001	2002	2003	2004	2005	2006
Violent Crimes	1,426,044	1,425,486	1,439,480	1,432,677	1,383,676	1,360,088	1,390,745	1,417,745

Uniform Crime Report data on the rate of violent crime also show a decline that began in the 1990s ending with small increases in 2005 and 2006. As shown in Chart 2, the overall rate of violent crime per 100,000 persons showed an increase of 1.3 percent from 2004 to 2005 and an increase of 1.0 percent from 2005 to 2006.

Chart 2 - Reported Violent Crime Rates, 1999 - 2006



	1999	2000	2001	2002	2003	2004	2005	2006
Violent Crimes	523	507	505	494	476	463	469	473

While the latest Uniform Crime Report data show that the number and rate of reported violent crimes were lower in 2006 than 5 years ago, the increases in violent crime over the past 2 years are troubling.

The National Crime Victimization Survey (NCVS) also measures national crime rates by surveying a representative sample of over 77,000 households on the frequency, characteristics, and consequences of criminal victimization, 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.

Since the September 11 attacks, the Department's law enforcement and prosecution components have shifted significant resources formerly devoted to crime prevention and control to focus on terrorism. For example, the OIG assessed the FBI's reallocation of resources in a September 2005 report and found that the Department was investigating and prosecuting significantly fewer traditional criminal matters than it did prior to September 11, 2001.

In that report, the OIG recommended that the FBI ensure that it has accurately evaluated its investigative needs and translate those assessments into realistic field agent allocations. In its most recent response, the FBI reported that it has been working to update its resource utilization practices to more precisely match its investigative needs. The FBI also said that it continues to modify its strategic planning methods to ensure that future resource allocations more closely meet field investigative demands. Specifically, in FY 2006 the FBI began a new strategic planning initiative called the Strategic Management System (SMS) to integrate strategic planning across operational and administrative areas. However, the FBI has not yet implemented SMS throughout all of its programs.

The FBI also has made progress in implementing our recommendations to enhance its coordination of identity theft, gang-related matters, fugitive apprehension, and alien smuggling. For example, since issuance of our report the FBI established a National Identity Theft Center Working Group staffed by personnel in several FBI divisions. The working group seeks to gather information from a variety of sources, analyze that information to identify trends, and distribute its analyses to FBI field offices and identity theft task forces, as well as to state and local law enforcement agencies.

In October 2006, the Department announced a 3-phase "Initiative for Safer Communities" to target violent crime prevention efforts in selected communities across America that have shown increases in crime. The first phase consisted of visits to 18 cities to learn about their crime problems and solutions. During the second phase, Department staff analyzed findings from the visits and identified three common themes: local gangs and street groups committing violent crimes, prevalence of gun crimes, and youth violence. The Initiative's third phase, announced by the Department in May 2007, consists of new efforts to enhance federal law enforcement efforts, assistance to state and local law enforcement, and requests to Congress to bolster legal authorities and funds for combating violent crime.

The Department's law enforcement components have implemented task forces and other initiatives to address aspects of the violent crime problem – DEA Mobile Enforcement Teams, FBI Safe Streets Task Forces, USMS Regional and District Fugitive Task Forces, and ATF's Violent Crime Impact Teams. In addition, since 2001 the Department has supported the Project Safe Neighborhoods initiative that seeks to reduce gun crime under the leadership of the U.S. Attorney in each federal district.

One of the Department's key challenges is to effectively coordinate its violent crime initiatives to ensure that they are complementary and do not waste resources through unnecessary duplication of effort. In addition, we believe the Department should continually assess the effectiveness of the various initiatives to determine if it is maximizing the impact of Department resources on reducing violent crime.

For example, a May 2007 OIG report found that coordination efforts among the Department's four law enforcement components were not fully effective at preventing duplication of efforts by these violent crime task forces. On a

positive note, the Department issued a new policy in May 2007 in response to the OIG report that requires all U.S. Attorneys to report to the Department on violent crime task force coordination efforts, coordination problems, and guidance or policies adopted or revised to address the problems. In addition, the Department implemented a requirement for components to obtain the Deputy Attorney General's approval before implementing new violent crime task forces in order to ensure coordination of these efforts.

In May 2006, the OIG reviewed ATF's implementation of its Violent Crime Impact Teams (VCIT), which seeks to decrease homicides and other violent firearm crimes in targeted urban areas. The OIG evaluation concluded that while the VCIT strategy may be an effective tool to reduce violent crime in target areas, there has been inconsistent application by ATF of key elements of the VCIT strategy. In light of ATF's planned expansion of the VCIT initiative from 25 to 30 cities in 2008, a specific challenge for the Department is to fully implement VCIT as designed and to evaluate VCIT and other violent crime task forces in order to gauge their effectiveness.

In addition to the operational assistance provided to state and local law enforcement agencies by the Department's task forces, OJP awards grants to support gang violent crime reduction efforts. For example, during FYs 2006 and 2007 OJP awarded $2.5 million to each of 10 cities to support prevention, enforcement, and offender reentry programs. As is discussed further in the Grant Management Challenge, proper oversight and evaluation is needed to ensure that these funds are being used for their intended purpose and that the activities they support are effective.

In sum, the Department faces a significant challenge in working with state and local law enforcement to address the recent rise in violent crime while shifting substantial resources from its criminal investigations to meet its counterterrorism-related responsibilities.

6. Detention and Incarceration: The Department's ability to safely and economically manage growing federal detainee and inmate populations presents a continuing management challenge. Among the key issues the Department needs to address in order to meet its goal of providing a safe, secure, and humane confinement environment are sufficient and economical prison and detention space, properly trained correctional officers, and appropriate management of high-risk inmates to protect the public from further criminal activities and to protect staff and inmates from harm.

The BOP is responsible for approximately 200,000 federal offenders, most of whom are housed in BOP-operated facilities. In FY 2007, the BOP received an appropriation of approximately $5.4 billion. Moreover, approximately 56,000 federal detainees awaiting trial or sentencing are housed each day by the USMS, primarily in jails under contract with the USMS. The Department's Office of the Federal Detention Trustee (OFDT) provides oversight of the USMS's detention activities and manages the budget for housing USMS detainees, which in FY 2007 was more than $1.2 billion.

Since FY 2002, the number of federal inmates has increased by 22 percent and the number of federal detainees by 40 percent. According to the Department's most recent strategic plan, the BOP expects to continue to grow by 5,000 inmates per year and projects that by 2012 the total inmate population will exceed 225,000, with BOP facilities experiencing an overcrowding rate of 28 percent.

Because the USMS houses only about 21 percent of its detainees in federal facilities, it is dependent on detention space leased from state and local governments to house the bulk of its detainees. According to OFDT estimates, the average daily population is expected to increase from the current 56,000 detainees to 63,145 in FY 2008. To house these federal detainees, the USMS has entered into more than 1,800 Intergovernmental Agreements (IGA) with state and local governments at an average daily rate of $63.22 or more than $1 billion per year. Consequently, a significant challenge for the Department is to obtain needed detention space for detainees without overpaying for it.

A March 2007 audit of the Department's oversight of the IGA program disclosed longstanding and significant deficiencies in how per-inmate costs paid by the Department were determined and monitored. Since 1995, the OIG

has audited 31 IGAs between the USMS and state and local governments for detention space and found almost $60 million in dollar-related findings. A recurring finding was that the USMS paid state and local governments significantly more than their actual and allowable costs for detention space. However, OFDT instructed the USMS not to seek recovery of the overpayments identified by the OIG. The OIG believes that this instruction was overbroad and the Department's Civil Division is currently reviewing certain individual OIG audits to determine whether legal action would be appropriate to recoup overpayments.

Going forward, OFDT is implementing an automated system known as eIGA to help determine the per-inmate daily reimbursement rate. The OIG believes that eIGA is a positive step toward improving the process that has historically been used to establish jail-day rates. However, the OIG also believes that OFDT should consider additional information as part of the eIGA formula so that the Department will be in the strongest possible position to negotiate with state and local jails to control costs. For example, as currently structured eIGA does not capture a jail's average daily population, indirect costs, or revenue generated from operations (also known as credits). The OIG believes this information is necessary to an accurate understanding of a detention facility's actual costs, and therefore has recommended that OFDT modify eIGA to capture this information so that it will be available to the USMS personnel charged with negotiating IGAs with state and local governments.

In May 2007, the OIG met with representatives from the Office of the Deputy Attorney General, OFDT, and the Justice Management Division to discuss the OIG's recommendation regarding eIGA. Since this meeting, the parties have been discussing the OIG's recommendations and refinement of the eIGA process. However, as of September 30, 2007, no resolution has been reached.

As part of its management of federal inmates and detainees, both the BOP and the USMS seek to ensure that they receive quality, cost-effective medical care. With the increasing population and rising medical costs, cost containment for medical services remains a challenge for the Department. For example, during the OIG's November 2005 audit of the BOP's pharmacy services, we found that the BOP's total health care costs for treating inmates increased from approximately $413 million in FY 2000 to approximately $624 million in FY 2004, an average annual increase of close to 11 percent. During that same period, the BOP's costs for prescription medications and related supplies increased an average of 23 percent annually, from $22.5 million in FY 2000 to $50.7 million in FY 2004. We concluded that the BOP could reduce prescription medication costs by controlling waste from unused prescriptions; fully implementing cost-savings initiatives such as requiring inmates to pay for over-the-counter medications; and maintaining accurate records of controlled substances and their administration. Since completion of the audit, the BOP has implemented the report's 13 recommendations.

In an ongoing audit, the OIG is examining the BOP's efforts to manage inmate health care costs and whether the BOP is effectively administering its medical services contracts effectively monitoring its medical services providers.

The USMS faces similar health care issues with detainees in its custody. In a February 2004 OIG audit, we concluded that the USMS was not effectively managing medical care of federal detainees. We found that the USMS failed to adequately track and monitor detainees with communicable diseases, failed to provide adequate emergency response to detainees, and failed to comply fully with statutory cost saving measures that resulted in the USMS paying approximately $7 million more annually than necessary for detainee medical care. In response to the audit, the USMS and OFDT have been negotiating a national managed health care contract. The USMS stated that its Technical Evaluations Board has completed evaluation of bids and plans to award the contract before the end of 2007.

An unresolved challenge for the Department is to ensure that its staff and other Department employees who work in the correctional environment benefit from appropriate safety precautions. Even though more than 15 months have passed since OIG Special Agent William "Buddy" Sentner was shot and killed by a BOP correctional officer who

brought a gun into a federal prison in Florida, the BOP has not yet implemented basic security measures such as requiring all staff to pass through a metal detector before entering a BOP facility.

Sexual abuse of inmates by BOP staff also remains a problem in BOP facilities. Approximately 12 percent of all OIG investigations throughout the entire Department are related to staff sexual abuse of inmates. An April 2005 OIG report highlighted the problem of sexual abuse of inmates and deficiencies in federal law that results in lenient sentences or unprosecuted cases. Congress enacted legislation in 2006 that increased the penalties and broadened federal jurisdiction for prosecuting staff sexual abuse of federal inmates. During FY 2008, the OIG plans to assess the effect of the statutory changes and the BOP's efforts to deter and detect staff sexual abuse of inmates.

The BOP also is responsible for monitoring the activities of inmates to ensure that they do not continue their criminal activities from prison. In a September 2006 report, we found significant shortcomings with the BOP's monitoring processes for terrorist inmates' mail, telephone calls, visits, and cellblock conversations. We also found that the Department did 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, the most restrictive conditions that can be placed on an inmate's communications.

Based on our recommendations, the BOP has made progress in improving its monitoring of terrorist inmates. For example, since issuance of our report the BOP stated that it is performing 100 percent monitoring of all terrorist inmates' written and telephone communications; conducting more foreign language and intelligence training for prison staff who perform the monitoring; and increasing the use of electronic tools such as language translation software and databases that facilitate intelligence analyses. The BOP also has established a Counterterrorism Unit to manage counterterrorism intelligence and language translation across its facilities and a Communications Management Unit in Terre Haute, Indiana, to house inmates who require increased monitoring of their communications. In addition, in August 2007 the Department developed new procedures to ensure that terrorist and other high-risk inmates are reviewed systematically to determine whether they should be placed under Special Administrative Measures during pretrial and post-conviction incarceration. Although we have not yet assessed the effect of these changes, we believe they represent significant steps to reduce the threat that inmates can continue during their incarceration.

7. Sharing of Intelligence and Law Enforcement Information: The Department continues to improve its sharing of law enforcement and intelligence information with federal, state, and local officials. However, ongoing efforts throughout the Department to upgrade information technology (IT) systems remain a key factor in the Department's ability to more fully meet this challenge.

The Department is moving forward with several broad initiatives to overcome barriers to information-sharing, including a program called the Law Enforcement Information-Sharing Program (LEISP). LEISP is a nationwide collaboration involving the FBI, other Department components, the Department of Homeland Security (DHS), the intelligence community, and local law enforcement agencies that seeks to enable law enforcement agencies to access Department information in a timely and secure manner. As part of the LEISP, OJP has awarded grants to examine the policy, connectivity, and jurisdictional issues that have hampered effective justice information-sharing in the past. In addition, through the Department's Global Justice Information Sharing Initiative, all Department components have adopted a common computer language for sharing information among differing computer systems. In FY 2006, the Department began requiring that state and local criminal justice agencies that receive federal grants use this information-sharing standard.

Several Department components are moving forward with other targeted information-sharing initiatives. For example, the DEA, in partnership with the High Intensity Drug Trafficking Area (HIDTA) Program and the Regional Information Sharing Systems (RISS), is developing the National Virtual Pointer System (NVPS). The NVPS will connect databases of participating federal, state and local law enforcement agencies into a single automated system to allow them to share information on their investigations. Through NVPS, participating

agencies can determine if any other law enforcement agency is investigating the same subject regardless of the crime. Future plans include migrating the NVPS into the FBI's National Law Enforcement Data Exchange (N-DEx). The FBI is developing N-DEx to enable law enforcement agencies to search, link, analyze, and share criminal justice information such as incident and case reports, incarceration data, and parole and probation data on a national basis. Participating agencies will be able to use N-DEx to detect relationships among people, places, and crime characteristics across jurisdictions. The Department anticipates completing the implementation of N-DEx by FY 2010.

Ongoing OIG reviews of the FBI's efforts to upgrade its IT systems have shown that the FBI has made progress in addressing deficiencies in its information-sharing capabilities. For example, a March 2006 OIG report on development of the FBI's Sentinel case management system 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, the OIG was concerned that Sentinel would not provide a common framework for other agencies' case management systems as initially intended. In a follow-up audit issued in December 2006, the OIG found that, based on OIG recommendations, the FBI has focused more attention on external information sharing needs and coordinating its requirements for Sentinel with the requirements of other Department agencies, DHS, and other federal entities. In addition, Sentinel is being built to meet the standards of the new National Information Exchange Model, a joint Department/DHS standard that has become the government-wide standard for any new law enforcement and intelligence systems being developed.

The successful completion of Sentinel remains a continuing challenge. With the most difficult phases of the project yet to come, the FBI must remain vigilant in monitoring Sentinel's development. In the most recent follow-up report issued in August 2007, the OIG noted progress in the management of Sentinel, including the FBI's implementation of its earned value management and risk management. However, as the FBI moves forward with development of Sentinel, it must ensure that it continues to implement these and other project management processes while incorporating lessons learned from the Sentinel development process.

In a separate audit, the OIG examined the progress of the Integrated Wireless Network (IWN), a $5 billion joint project among the Department, the DHS, and the Department of Treasury that is intended to address federal law enforcement requirements to communicate across agencies, allow interoperability with state and local law enforcement partners, and meet mandates to use federal radio frequency spectrum more efficiently. The OIG concluded that the IWN project was at a high risk of failure. Despite over 6 years of development and more than $195 million in funding, the OIG concluded that the IWN project does not appear to be on the path to providing the intended seamless interoperable communications system. The causes for the high risk of project failure include uncertain and disparate funding mechanisms for IWN, the fractured partnership between the Department and DHS on IWN, and the lack of an effective governing structure for the project.

As mentioned previously in the Violent Crime challenge, a May 2007 OIG report assessed the coordination of investigations conducted by four Department violent crime task forces. This review examined not only the Department's coordination of its task force investigations, but also the use of information-sharing systems to prevent duplication of effort by the various task forces. We found that U.S. Attorneys and local task force managers in some cities used information-sharing systems, such as HIDTA, to increase coordination of task force operations. However, in other cities task forces did not use information-sharing systems and conducted duplicate investigations and wasted resources. In response to OIG recommendations, the Deputy Attorney General directed Department components to adopt a policy requiring the use of information-sharing and deconfliction measures to coordinate investigations in areas where more than one Department-led violent crime task force operates.

In sum, the Department continues to make progress in improving its ability to share a greater range of law enforcement and intelligence information, both within the Department and with other federal, state, and local law enforcement agencies. Nevertheless, the Department's efforts to upgrade its IT systems remain a key factor in its

ability to more fully meet this information-sharing challenge, and the Department still faces significant challenges to ensure the timely, effective, and secure sharing of vital intelligence and law enforcement information.

8. Information Technology Systems Planning, Implementation, and Security: As noted in other challenges, the Department's efforts to upgrade critical IT systems in a timely and cost-effective manner have produced mixed results. In the past, widespread problems ranging from a lack of critical managerial processes to mismanagement of individual systems have hobbled attempts by the Department to upgrade critical IT systems. While the Department is now making positive strides in various areas, several major IT projects such as the Unified Financial Management System, the Litigation Case Management System, and the IWN project remain at risk in terms of cost, schedule, and performance.

The OIG also is concerned the Department lacks the ability to accurately track the cost of its major IT systems and, more fundamentally, that it does not exercise 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 provide 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.

We also are concerned about the excessive reliance the Department places on contractors to develop, monitor, and run internal Department systems. We have found numerous systems run by contractors in which Department employees do not always understand either the mechanics or the overall processes required to make the systems perform as intended. For example, OIG audits of the Terrorist Screening Center and the Department's watchlisting processes found that contractors are performing a significant portion of the information system management and data analysis.

Notwithstanding these concerns, we note that several DOJ components have made significant progress during the past year to improve their IT management practices. One component in particular that appears to be learning from past mistakes is the FBI. As discussed above, based on a variety of recent reviews we believe the FBI is making progress in its efforts to develop the modern IT systems needed to perform its mission and provide its employees with the ability to effectively analyze and share the vast amount of information it collects. Over the past several years, the FBI has instituted better IT management processes and controls through its Life Cycle Management Directive. Continuity in both the FBI's CIO position and its project management staff – a huge problem in failed previous efforts – also has stabilized. In addition, all of the FBI's IT activities have been centralized under the FBI CIO, who now controls all agency IT spending.

The Department also faces the challenge of assuring that the more than $2 billion it receives annually for the Department's IT systems is being spent effectively. A June 2007 OIG report examined the Department's inventory of IT systems and identified 38 major IT systems estimated by system mangers to cost over $15 billion through 2012. The OIG's audit found that the cost information the Department provides on its IT systems to Congress, OMB, and senior management within the Department is unreliable. Specifically, IT system cost reporting within the Department is fragmented, uses inconsistent methodologies, and lacks control procedures necessary to ensure that cost data for IT systems is accurate and complete. In our opinion, the lack of complete and verifiable cost data undermines the effectiveness of oversight of IT projects by various entities, including the Department's Investment Review Board, Department and component CIOs, Congress, and OMB.

In an August 2007 report, we inventoried approximately 800 studies, plans, and evaluations of component IT systems. Our audit found that components do not prepare many of the required IT studies, plans, and evaluations. Based on the limited number of certain types of plans and evaluations produced on major systems and projects, we recommended that the CIO evaluate why project teams do not prepare certain plans and evaluations, reassess the

utility of those documents, and consider revising the standards for producing IT studies, plans, and evaluations for individual IT projects. The CIO concurred and has initiated the evaluation.

As the Department develops new IT systems, it also must ensure the security of those systems and the information they contain. 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 IT security audits in response to the Federal Information Security Management Act. These audits have noted improvement in the Department's information security over time, but we also have 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. In response to our specific findings, the Department has made improvements in its oversight of IT security. For example, Department components are testing their 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.

In sum, if the Department is to build on the advances it has made in IT systems planning, implementation, and security, it must closely manage these projects to ensure the systems are cost-effective, well-run, secure, and successful in achieving their objectives.

9. Civil Rights and Civil Liberties: A continuing challenge for the Department is to balance aggressive pursuit of its counterterrorism responsibilities with the need to protect individual privacy rights and civil liberties. This year, the OIG found significant problems in this challenge in an important area. A March 2007 OIG review reported on serious misuse by the FBI of national security letters (NSL). NSLs are used in terrorism and espionage investigations to obtain from third parties, without a court order, records such as telephone toll billing records, electronic communication transactional records, financial records, and credit information.

In the USA PATRIOT Improvement and Reauthorization Act of 2005 (Patriot Reauthorization Act), Congress directed the OIG to report on the FBI's use of NSLs and Section 215 orders for business records. The USA PATRIOT Act (Patriot Act), enacted in 2001, significantly expanded the FBI's preexisting authority to obtain information through NSLs. The Patriot Act lowered the threshold standard for issuance of NSLs, allowed FBI field office Special Agents in Charge to approve issuance of NSLs, and permitted the FBI to use NSLs to obtain consumer full credit reports in international terrorism investigations. In addition, section 215 of the Patriot Act allows the FBI to seek an order from the Foreign Intelligence Surveillance Court to obtain "any tangible thing," including books, records, and other items from any business, organization, or entity if the item is for an authorized investigation to protect against international terrorism or clandestine intelligence activity.

The OIG issued reports in March 2007 that examined the FBI's use of NSLs and Section 215 orders to obtain business records. While Section 215 did not create any new investigative authority, it significantly expanded existing authority by broadening the types of records that can be obtained and by lowering the evidentiary threshold to obtain an order. Public concerns about the scope of this expanded authority centered on the FBI's ability to obtain library records. The OIG report found that the FBI did not obtain Section 215 orders for any library records during the 2002 to 2005 period covered by our review. In addition, the OIG review did not identify any instances involving improper or illegal use of pure Section 215 orders.

However, the OIG's 126-page report on NSLs revealed a much different picture. The OIG's review detailed significant improper or illegal uses of NSL authorities from 2003 through 2005, including violations involving the issuance of NSLs without proper authorization, improper requests under the statutes cited in the NSLs, and unauthorized collection of telephone or Internet e-mail transactional records. The OIG also identified many instances in which the FBI improperly obtained telephone toll billing records pursuant to more than 700 so-called "exigent letters" signed by personnel in the FBI's Counterterrorism Division without first issuing NSLs. The OIG

found that the FBI's acquisition of this information circumvented the requirements of the NSL statute, violated the Attorney General's Guidelines, and contravened internal FBI policy. We also found that the FBI issued some of these "exigent letters" in non-emergency circumstances, failed to ensure that there were duly authorized investigations to which the requests could be tied, and failed to ensure that NSLs were issued promptly after the "exigent letters" were sent. Moreover, the letters inaccurately represented that the FBI had already requested subpoenas for the information when, in fact, it had not.

The OIG's March 2007 report made 10 recommendations to the FBI relating to its use of NSLs, including improving its database to ensure that it captures timely, complete, and accurate data; issuing additional guidance to field offices to assist in identifying possible intelligence violations arising from the use of NSLs; and taking other steps to ensure that the FBI uses NSLs in accordance with the requirements of national security letter authorities, Attorney General Guidelines, and internal FBI policies. The FBI concurred with all of the OIG's recommendations and agreed to implement corrective actions.

The FBI and the Department began taking other actions in response to the problems disclosed in the OIG's March 2007 report. The Attorney General directed the Department's National Security Division (NSD) and the Privacy and Civil Liberties Office to work with the FBI to implement corrective actions. For example, the FBI conducted a retrospective audit of a random sample of NSLs issued from 2003-2006 by the FBI's 56 field offices and Headquarters Divisions to check for possible intelligence violations or violations of Attorney General Guidelines or internal policies governing the use of NSLs. In addition, in March 2007 the FBI prohibited the use of so-called "exigent letters" with the promise of future legal process to obtain telephone toll billing or subscriber information from telephone companies. In September 2007, the Department established an oversight section within the NSD to review the FBI's use of NSLs and other national security tools. The FBI also created an Office of Integrity and Compliance to promote FBI compliance with laws, rules, and regulations not only in the FBI's National Security Branch but in all FBI programs and activities.

The challenge for the Department and the FBI is to conduct continuous, meaningful oversight of the FBI's use of these important but intrusive authorities. In addition, integration of the FBI's Office of Integrity and Compliance into the culture and structure of the FBI presents a challenge that will require substantial resources and wide support from managers throughout the FBI.

The OIG is currently conducting a follow-up review on the FBI's use of NSLs that focuses on three areas: the FBI's use of NSLs in calendar year 2006 (as directed by Congress in the Patriot Reauthorization Act), the FBI's and Department's implementation of the OIG's recommendations from our March 2007 NSL report and other corrective measures, and the FBI's use of "exigent letters."

In addition to NSLs, the OIG continues to actively review other Department programs affecting civil rights and civil liberties. For example, the OIG is reviewing the Department's involvement with the National Security Agency program known as the "terrorist surveillance program." This ongoing review is examining the Department's controls and use of information related to the program and the Department's compliance with legal requirements governing the program.

During the past year, the Department made progress in addressing the final outstanding recommendation from an earlier OIG report, the June 2003 report entitled, "The September 11 Detainees: A Review of the Treatment of Aliens Held on Immigration Charges in Connection with the Investigation of the September 11 Attacks." In that report, the OIG examined the treatment of these detainees, including circumstances surrounding their detention, their access to counsel, the timing of their release from custody or removal from the United States, and their conditions of confinement. The OIG report found significant problems in the way the Department handled the September 11 detainees, and included 21 recommendations related to issues under the jurisdiction of the FBI, the BOP, and the Department, as well as immigration issues now under the jurisdiction of the DHS. In July 2007, the Department and the DHS finally entered into a memorandum of understanding (MOU) to formalize policies,

responsibilities, and procedures for managing a national emergency that involves alien detainees. We believe that full implementation of the MOU procedures could help prevent many of the problems we uncovered in our September 11 detainee review.

In sum, striking the appropriate balance between meeting its critical counterterrorism-related responsibilities and respecting civil rights, civil liberties, and privacy rights remains a key challenge for the Department.

10. Cybercrime: Cybercrime involves the use of computers to conduct criminal activity such as fraud, identity theft, theft of intellectual property, copyright infringement, and sexual exploitation of minors. 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 opportunity for cybercrime increases with the growth of the Internet. Every day, criminals are invading homes and offices across the nation – not by breaking down windows and doors, but by breaking into laptops, personal computers, and wireless devices. For example, 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 207,492 complaints in 2006. These included fraud-related complaints such as credit or debit card fraud, as well as non-fraud related complaints such as computer intrusions, spam or unsolicited e-mail, and child pornography.

Cybercrime also poses a threat to U.S. national economic and security interests. According to a 2005 FBI survey, the overall loss from computer crime was estimated at $67.2 billion annually for U.S. organizations. The estimated loss associated with identity theft was $49.3 billion in 2006 and approximately $1 billion due to "phishing." Phishing is a high-tech scam that frequently uses unsolicited messages to deceive people into disclosing financial or personal identity information.

Another challenge facing the Department is the threat posed to the nation's national security through attacks on our computer-reliant critical infrastructures and theft of sensitive information. Over the past several years the Department has taken a number of positive steps to address the varied facets of cybercrime. For example, in 2002 the FBI created a Cyber Division at FBI headquarters to manage and direct its overall cybercrime program in light of the international aspects and national economic implications of cyber threats. In March 2003, the FBI issued the Cyber Division National Strategy, which describes four objectives for identifying and neutralizing individuals or groups conducting computer intrusions and spreading malicious computer code, intellectual property thieves, Internet fraud, and on-line predators that sexually exploit or endanger children.

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 7 years and now numbers approximately 40 attorneys.

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 2007, more than 200 attorneys throughout the country have been assigned to the CHIP program.

Established in May 2006, the Department's "Project Safe Childhood" seeks to protect children from sexual abuse and exploitation on the Internet. The project, led by the 94 United States Attorneys, developed regional task forces to investigate and prosecute crimes against children committed on the Internet or through other electronic media and

communications devices. The project seeks to integrate federal, state, and local efforts; increase the number of cases prosecuted in federal court where stiffer punishment is available; provide training to law enforcement partners to more effectively investigate and prosecute these cases; and increase community awareness of this problem in order to provide tools to parents and children seeking to report possible violations.

In sum, the Department and its components have taken steps to address the varied facets of cybercrime. While the Department has developed several initiatives to combat aspects of this complicated crime, the Department must continue to respond to this growing challenge.