November 13, 2008

MEMORANDUM FOR THE ATTORNEY GENERAL
THE DEPUTY ATTORNEY GENERAL

FROM: GLENN A. FINE
INSPECTOR GENERAL

SUBJECT: Top Management and Performance Challenges in the Department of Justice – 2008

Attached to this memorandum is the Office of the Inspector General's (OIG) 2008 list of top management and performance challenges facing the Department of Justice (Department). We have prepared similar lists since 1998. By statute, this list is 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. We hope that this document will assist 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

Top Management and Performance Challenges in the Department of Justice – 2008

1. Counterterrorism: The Department's top priority remains its ongoing efforts to detect and deter terrorism. Seven years after the September 11 terrorist attacks, the Department of Justice (Department) in general and the Federal Bureau of Investigation (FBI) in particular are taking positive steps to address gaps in their tools to detect and deter terrorism, but continuing issues demonstrate the significant challenges the Department still faces in this area.

For example, in March 2008 the Office of the Inspector General (OIG) reported on the Department's processes for nominating known or suspected terrorists to the consolidated terrorist watchlist. We found that watchlist nominations from FBI field offices often were incomplete or contained inaccuracies, which caused delays in the nominations process. We also found that FBI case agents did not always update watchlist records when new information became known, and did not always remove watchlist records when appropriate. Moreover, while the FBI has developed a formal policy for nominations of individuals to the watchlist, no standard nominations policy existed for other Department components involved in watchlisting. We made seven recommendations regarding nominations to the consolidated terrorist watchlist and the sharing of terrorism-related information. The FBI and other Department components agreed with the recommendations in this report, and in October 2008 the Department issued a department-wide policy designed to ensure consistent and appropriate handling of watchlist information. The new policy requires all Department components to share terrorism information with the FBI and establishes the FBI as the only component with the authority to make watchlist nominations on behalf of the Department.

As a follow-up to this report, we are now examining the FBI's actual watchlist nomination practices. In this review, we are performing an in-depth analysis of whether subjects of FBI cases are appropriately and timely watchlisted, whether subjects of FBI investigations are removed from the consolidated terrorist watchlist in a timely manner when appropriate, and whether the individuals who are not subjects of open terrorism investigations are being watchlisted by the FBI.

In another ongoing follow-up review, the OIG is examining the FBI's Foreign Language Services Program. The FBI's ability to timely translate the large amount of foreign language materials it regularly collects is critical to national security. As the FBI focuses on its two highest investigative priorities – counterterrorism and counter intelligence – it must rely heavily on its translation resources. OIG audits of the FBI's Foreign Language Services Program in 2004 and 2005 identified significant deficiencies in its translations of the materials it collects in foreign languages. Our audits found a continuing backlog of unreviewed foreign language material, some instances where high-priority material had not been reviewed within 24 hours in accord with FBI policy, the lack of full implementation of a quality control program for linguists, and continuing challenges in meeting linguist hiring goals. The ongoing OIG audit is examining the current state of the FBI's foreign translation efforts, whether a backlog still exists, and the

actions taken by the FBI to address any backlog. We are also examining the FBI's efforts to ensure appropriate prioritization of translation work, accurate and timely translations of pertinent information, and proper security of sensitive information.

Past OIG reviews also found that the FBI's counterterrorism and intelligence-gathering efforts have been hampered because of outdated information technology (IT) systems. In recent years the FBI has made significant progress in improving management of its IT program (which we discuss in more detail under the IT systems implementation challenge). However, the FBI will not benefit from a fully functional case management system for several more years.

Another critical aspect of the Department's counterterrorism responsibilities is balancing the need for effective counterterrorism measures with the need to appropriately protect civil rights and civil liberties. In the past, when obtaining enhanced authority in using certain counterterrorism tools, the FBI has not always ensured that it complied with the legal requirements accompanying these news tools. A particularly salient example is the FBI's use of national security letters (NSL). Our first report on the FBI's use of NSLs, issued in March 2007, found serious and widespread misuse of these authorities, including NSLs being issued without proper authorization, improper requests under the NSL statutes, and unauthorized collection of telephone or Internet e-mail transactional records.

Our March 2008 follow-up review found that the FBI and the Department had made significant progress implementing the recommendations in our first report and adopting corrective actions to address the serious problems we identified. For example, the FBI has implemented a new NSL data system to facilitate the issuance and tracking of NSLs and improve the accuracy of its reports to Congress and the public on NSL usage. The FBI also issued guidance to its agents on the proper use of NSLs, and conducted training of field and headquarters personnel.

Another important response to the OIG's findings on the FBI's misuse of NSL authorities is the FBI's creation of a new Office of Integrity and Compliance (OIC), modeled after private sector compliance programs. The OIC's mission is "to develop, implement, and oversee a program that ensures there are processes and procedures in place that promote FBI compliance with both the letter and spirit of all applicable laws, regulations, and policies." According to the FBI, the OIC will periodically examine major compliance risks among FBI programs, subject those risks to detailed risk assessments, develop compliance checklists to guide reviews of these risks, and develop and implement risk mitigation plans. However, we recommended that the FBI consider providing the OIC with a substantial permanent staffing level so that this office would develop the skills, knowledge, and independence to lead or directly carry out the new compliance program.

In addition, the Department's National Security Division now conducts periodic national security reviews of FBI field and Headquarters divisions to assess whether the FBI is using various intelligence techniques, including NSLs, in accordance with applicable laws, guidelines, and policies. However, we believe that the Department and the FBI must aggressively monitor compliance with NSL authorities and ensure that adherence to these and other legal requirements are permanently imbedded in FBI culture and practice.

By its very nature, the Department's counterterrorism responsibilities also require close coordination with other parts of the Intelligence Community and, in some cases, the military. In May 2008, the OIG issued a report that examined the FBI's role in, and observations of, detainee interrogations in Guantanamo Bay, Afghanistan, and Iraq. Among other things, the OIG review examined whether FBI agents participated in any detainee abuse, witnessed incidents of detainee abuse in the military zones, or reported alleged abuse to their superiors or others. The OIG found that the vast majority of the FBI agents deployed in the military zones separated themselves from other agency interrogators who used techniques not permitted by the FBI, and that FBI agents continued to adhere to FBI interrogation policies. However, some FBI agents witnessed interrogation techniques by other agencies that FBI agents believed were abusive. A few of these FBI agents' reports reached senior-level officials in the Department of Justice and were the focus of inter-agency discussions. However, we found no evidence that the FBI's concerns affected other agencies' interrogation policies.

We also found that the FBI did not fully or timely respond to repeated requests from its agents in the military zones for guidance regarding several issues related to detainee interrogations. We recommended that the FBI supplement the guidance it provided in May 2004 to address the circumstances under which FBI agents may participate in interviews of detainees who have previously been subjected to non-FBI interrogation techniques, as well as the circumstances under which the FBI may use information obtained from detainees by other agencies through the use of non-FBI techniques. We also recommended that the FBI consider supplementing its guidance regarding when agents should report the conduct of other agencies' interrogators. The FBI's response to these recommendations remains outstanding.

With regard to other Department components, compared with several years ago we have seen substantially more focus on information sharing about counterterrorism issues. For example, the Federal Bureau of Prisons (BOP) has created a Counterterrorism Unit to assist in monitoring federal prisoners believed to have links to terrorist organizations and to enhance information sharing about these inmates. In addition, the Intelligence Program Manager for the Executive Office for United States Attorneys (EOUSA) spends 2 to 3 days per week on-site at the BOP unit, which has significantly improved intelligence sharing and communication between the BOP and U.S. Attorneys' Offices.

Moreover, in response to an OIG recommendation, the Department has issued interim guidance requiring a coordinated review between the FBI and U.S. Attorneys' Offices for each newly incarcerated pretrial or convicted BOP inmate associated with terrorism to determine the applicability of Special Administrative Measures (SAMs). Under SAMs, the inmates' mail, telephone calls, and visits are more closely monitored.

With respect to domestic terrorism, we are currently evaluating the coordination of explosives investigation activities between the FBI and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). Both the FBI and ATF have the authority to investigate explosive-related cases, but historically they have had significant disputes over their respective jurisdictions. Prior to the integration of ATF into the Department of Justice in 2003, each agency had developed its own investigative strategies and priorities, operated separate intelligence systems, and used different systems for reporting and measuring performance. Even after ATF's entry into the

Department and issuance of an Attorney General memorandum in August 2004 addressing several explosive-related jurisdictional issues, disputes between the two agencies have continued. As a result, our ongoing audit is reviewing ATF and FBI coordination on explosives-related cases, information sharing, laboratory services, and training.

In sum, the Department continues to enhance its counterterrorism efforts, but the Department still faces significant challenges in this area.

2. Sharing of Intelligence and Law Enforcement Information: The Department continued its efforts during the past year to improve its capacity to share law enforcement and intelligence information among Department components and with other federal, state, and local officials. On October 31, 2007, the President issued the National Strategy for Information Sharing (Strategy), which established a framework for information sharing among federal, state, and local government agencies, as well as with the private sector and foreign partners. One key element of the Strategy is to develop the 71 "fusion centers" established nationwide into a national integrated network to maximize law enforcement agencies' ability to detect, prevent, investigate, and respond to criminal and terrorist activity. To support implementation of this Strategy, the FBI assigned 250 personnel to 48 of the fusion centers, including 96 Special Agents, 119 Intelligence Analysts, and 35 specialized language or financial experts. In addition, U.S. Attorneys' Offices, the DEA, and ATF have assigned agents and anti-terrorism personnel to work at the fusion centers part-time.

However, while information sharing strategies are important, the implementation of new or upgraded information technology (IT) systems to facilitate information sharing remains a key factor in the Department's ability to meet this challenge. Over the past several years the Department has developed and is implementing plans for improving information sharing policies and practices, and has established the Law Enforcement Information Sharing Program (LEISP) as the single, coordinated law enforcement data and information sharing initiative for the entire Department. DOJ component information sharing initiatives should be consistent with, and support implementation of, the LEISP strategy. Two key information systems within LEISP are known as OneDOJ and the National Data Exchange (N-DEx). OneDOJ serves as a central repository for federal law enforcement data to be shared with other federal, state, local, and tribal entities. N-DEx is designed to be a national criminal law enforcement information sharing system available to the entire law enforcement community that will include information from federal, state, local, and tribal law enforcement agencies. One-DOJ and N-DEx promote information sharing by providing participating agencies with access to other agencies' law enforcement and intelligence information. The Department plans to integrate the two systems by February 2010.

In addition, as part of its support to the fusion centers, the FBI installed the FBI Network (FBINet), the FBI's centralized network management system to access its administrative, financial, and investigative systems, in 31 of the 71 fusion centers as of September 2008. The FBI plans to install FBINet in 18 additional centers by the end of December 2008.

The Department is taking other actions to facilitate information sharing. 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 fiscal year (FY) 2006, the Department began requiring that state and local criminal justice agencies that receive federal grants use this information-sharing standard. And in January 2008 the Department released new guidance on the National Information Exchange Model that establishes standards for data and system design to enable federal, state, and local criminal justice agencies to consistently share data.

In August 2008, the FBI issued its National Information Sharing Strategy and announced the selection of its first Chief Information Sharing Officer (CISO)/Senior Intelligence Officer for Information Sharing. The FBI CISO will be the FBI's designated senior official for information sharing and will lead the planning and coordination of all FBI information sharing initiatives.

The Department is providing significant funding for these and other information sharing projects. For example, in FY 2008 the Department's Justice Information Sharing Technology (JIST) initiative received $80.5 million. The JIST was established in FY 2006 as a centralized fund under the control of the Department's Chief Information Officer to ensure that investments in information sharing technology and infrastructure enhancements are aligned with the Department's overall IT strategy and enterprise architecture. The JIST account provides funding to support the continued development, implementation, or operation of various Department IT systems, including LEISP, the Litigation Case Management System (LCMS), Secure Identity Management & Communication (SIMC), the Unified Financial Management System (UFMS), the Justice Consolidated Office Network (JCON), and the Joint Automated Booking System (JABS).

During the past year, the OIG assessed the status of various information sharing systems within the Department and found significant progress. For example, our reviews of the FBI's efforts to upgrade its IT systems have found that the FBI has made progress in addressing deficiencies in its information-sharing capabilities. However, the successful completion of the FBI's Sentinel system remains a continuing challenge, with the most difficult phases of the project yet to come.

In addition, a June 2008 OIG audit examined the FBI's National Name Check Program and the Integrated Automated Fingerprint Identification System (IAFIS). These FBI programs provide federal agencies, state and local law enforcement agencies, and approved non-governmental institutions with criminal history and identification services from the FBI's vast repositories of investigative records. We found that the name check process used by the FBI has serious deficiencies, including relying on outdated and inefficient technology, personnel with limited training, overburdened supervisors, and inadequate quality assurance measures. Those deficiencies have resulted in large backlogs, with over 327,000 name check requests pending as of March 2008, a backlog that hampers timely adjudication of immigration applications. In addition, security check delays can slow the adjudication and deportation of applicants who may pose a national security threat to the United States. In contrast, we found that the FBI is able to accurately process millions of fingerprint checks through IAFIS, usually within 24 hours.

An ongoing OIG audit is examining the FBI's terrorist threat tracking system called Guardian. Originally implemented in 2004, Guardian is an automated system that has become the cornerstone of the FBI's terrorist threat assessment process for supporting the identification, collection, management, evaluation, analysis, and dissemination of all leads relating to terrorist threats and suspicious incidents, up to the secret classification level, within the FBI. Guardian also provides the FBI with the ability to share investigative data to support intelligence analyses and share investigative data with other government agencies. From July 2004 through November 2007, approximately 108,000 potential terrorism-related threats, reports of suspicious incidents, and terrorist watchlist encounters were entered into Guardian. The FBI determined that the overwhelming majority of the threat information documented in Guardian had no nexus to terrorism, but the FBI initiated over 600 criminal and terrorism-related investigations from October 2006 to December 2007. However, our review found that the FBI's use and maintenance of its Guardian system could be improved in several ways. For example, the FBI needs to better ensure the accuracy, timeliness, and completeness of the information entered in Guardian. Additionally, we found that the Guardian system requires better oversight and updates to improve its functionality and value.

To facilitate the sharing of threat and suspicious incident information between the FBI and its law enforcement partners that do not have access to Guardian, the FBI is also developing a web-based application called E-Guardian. This new system will allow sharing of terrorist threat reporting and threat information tracking among Fusion Centers, Joint Terrorism Task Forces, and state, local, and tribal law enforcement agencies. The E-Guardian system is intended to allow the FBI and state and local law enforcement to collect, share, and analyze threat and suspicious activity data electronically.

In sum, the Department has made significant 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. Yet, the Department's efforts to upgrade its IT systems remain a key challenge for the Department to more fully meet its need to share information.

3. Information Technology Systems Planning, Implementation, and Security: The Department continues to face the challenge of ensuring that the more than $2 billion it spends on Department's IT systems is being used effectively to implement and upgrade the Department's many IT systems.

One challenge is to simply report accurately the amount of money spent on IT systems. 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. Yet, the OIG audit found that the cost information the Department provides on its IT systems to Congress, the Office of Management and Budget (OMB), and senior Department management 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. Our audit concluded that 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 Chief Information Officers (CIO), Congress, and OMB. Since our report was issued, Department finance and IT officials have been assessing the feasibility of using the forthcoming Unified Financial Management System for capital planning and investment cost reporting for IT projects.

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 Department's 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 initiated an evaluation, but later determined that a coordinated review of the Department's System Development Life Cycle (SDLC) guidance was needed to address the recommendation. The CIO stated that he plans to complete this review in FY 2009, and he designated in May 2008 key studies, plans, and evaluations as mandatory for all development and major enhancement programs managed under the Department's SDLC.

The Department's recent efforts to upgrade critical IT systems in a timely and cost-effective manner have also produced mixed results. In the past, problems ranging from a lack of critical managerial processes to mismanagement of individual systems have hampered attempts by the Department to upgrade critical IT systems. While the Department is now making positive strides in a variety of areas, several major IT projects such as the Unified Financial Management System, the Litigation Case Management System, and the Integrated Wireless Network (IWN) still remain risky in terms of cost, schedule, and performance.

The OIG continues to be concerned that the Department does not exercise direct control over IT projects among Department components. Historically, the Department's components have resisted centralized control or oversight of major IT projects, and the Department's CIO does not have direct operational control of Department components' IT management. We believe the Department should enhance the CIO's oversight of the development of high-risk IT systems.

As the Department develops new IT systems, it also must ensure the security of those systems and the information they contain. For example, the Department must balance the need to share intelligence and law enforcement information with the need to ensure that such information sharing meets appropriate security standards.

The Department has made significant progress in the area of IT security. In May 2008, the Department received an A^+ from the House Committee on Oversight and Government Reform on its Federal Information Security Management Act (FISMA) report card, a grade reflective of the Department's well documented security policies and procedures.

However, this grade does not reflect actual implementation of those policies and procedures. In fact, OIG audits of the Department's information security conducted pursuant to FISMA have

identified continuing weaknesses with the Department's management, operational, and technical controls for its classified and sensitive but unclassified systems. Specifically, we found that the Department lacks effective methodologies for tracking the remediation of IT vulnerabilities identified in monthly system configuration scans, applying Department-wide remedies for known vulnerabilities, and conducting an inventory of devices connected to the Department's various IT networks.

In our reviews of individual systems, we have also found weaknesses in data security or IT systems in need of improvement. For example, in January 2008 the OIG issued a report on the Department's Victim Notification System (VNS), an automated system operated by the Executive Office for U.S. Attorneys (EOUSA) that notifies federal crime victims regarding developments in their cases. Our audit found insufficient internal controls to ensure the accuracy and completeness of data in the VNS. We also identified deficiencies in the security of VNS information, most notably that sensitive crime victim information contained within the VNS was not adequately protected. The OIG made 19 recommendations to help improve management of the VNS, including matters related to information technology. EOUSA concurred with our recommendations and has outlined a plan to address them.

As discussed in the "Sharing of Intelligence and Law Enforcement Information" challenge, we examined the FBI's National Name Check Program and the Integrated Automated Fingerprint Identification System as part of our audit of the FBI's security check procedures for immigration and naturalization applicants. We found that the FBI's name check processes rely on outdated and inefficient technology. While the FBI has explored some electronic tools to assist in the name check search process, it has not conducted a technical assessment of its phonetic name-matching algorithm, the key component in the name-matching system, which matches names to the FBI's index of names in its investigative files. We concluded that the FBI's algorithm is largely outdated and potentially ineffective, increasing the risk that submitted names are not accurately searched and matched against FBI files. While the FBI told us that it lacked adequate funding to implement technological improvements in its name check process, the OIG report noted that the FBI had not raised its name check fees in 17 years and thus lost opportunities to enhance its antiquated automated systems.

In contrast to our findings on the FBI's name check program, we determined that the FBI's automated fingerprint identification system is generally able to process millions of fingerprint submissions in an accurate and timely manner because of the fingerprint system's enhanced technology, well-trained personnel, and efficient tracking mechanisms.

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 able to achieve their objectives.

4. Civil Rights and Civil Liberties: As noted above, the Department faces the continuing challenge of balancing aggressive pursuit of its counterterrorism responsibilities with the protection of individual civil rights and civil liberties. FBI Director Mueller characterized this balance aptly in a May 2008 speech when he stated: "In the end, if we in the FBI safeguard our

civil liberties but leave our country vulnerable to terrorist attack, we have lost. If we protect America from terrorism but sacrifice our civil liberties, we have also lost."

During the past year, the Department and the FBI have taken steps to improve their use and oversight of intelligence authorities that we found have been misused in the past. As noted above in the counterterrorism challenge, in March 2007 the OIG issued a report examining the FBI's use of NSLs from 2003 through 2005, as well as its use of 215 orders to obtain business records from 2002 through 2005. We found significant misuses of NSLs, including 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, including records with data beyond the time period requested in the NSLs.

In March 2008, we completed a follow-up report, which examined the use of these authorities in 2006. This review also assessed the corrective actions by the FBI and the Department to address the serious misuse of NSLs that our first report detailed.

We found in this follow-up report that the FBI and Department made significant progress in implementing the recommendations contained in our first report and in adopting additional corrective measures to address the serious problems in NSL usage and oversight we had identified. Based on our review, we concluded that the FBI's leadership is committed to correcting the serious deficiencies in the FBI's use of NSLs and is stressing throughout the FBI the urgent need to adhere to the rules governing the use of NSL authorities.

Yet, while we found that the FBI and the Department have taken positive steps to address the issues that contributed to the serious misuse of NSL authorities, additional work remains to be done. For example, the Department's Office of the Chief Privacy and Civil Liberties still has not revised its initial proposal and considered further whether and how to provide additional privacy safeguards and measures for minimizing the retention of NSL-derived information. In addition, it remains to be seen whether the FBI's new Office of Integrity and Compliance will be effective in detecting and correcting non-compliance with the rules governing the intrusive techniques available to the FBI.

The OIG also is in the process of completing a related investigation into the FBI's use of "exigent letters." Our first NSL report uncovered this practice by which the FBI improperly obtained telephone toll billing records from three communication service providers pursuant to more than 700 letters requesting the information by citing exigent circumstances and claiming that grand jury subpoenas had been requested and would be served expeditiously. We found that grand jury subpoenas often were not contemplated or issued, and that in many cases there was no exigency at all. We concluded that these exigent letters circumvented the requirements of the Electronic Communications Privacy Act and violated Attorney General Guidelines and internal FBI policy. The FBI has since discontinued the use of exigent letters. The OIG's ongoing investigation is examining who was responsible for the use of exigent letters and other improper requests for telephone records.

The OIG also is examining other Department programs that affect 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.

As noted in the counterterrorism challenge, the OIG also has examined the FBI's management of the consolidated terrorist watchlist. We found in our March 2008 audit that the FBI had established criteria and quality controls to assist in developing proper and accurate watchlist nominations. While it is important to place names on the watchlist when appropriate, it is also important to remove names from the list when they should not be there. Our audit found that FBI case agents did not always update watchlist records when new information became known and that the FBI did not always remove watchlist records when it was appropriate to do so.

As illustrated by the OIG's oversight work in this area, striking the appropriate balance between meeting critical counterterrorism-related responsibilities while respecting civil rights and civil liberties remains a key challenge for the Department.

5. Restoring Confidence in the Department of Justice: An ongoing challenge is the need to restore public confidence in the integrity of Department operations in light of concerns about politicized hiring in the Department. Related to this challenge is the need to prepare for an orderly transition to new Department leadership when the Administration changes in early 2009.

In the past several years, the Department has been faced with serious allegations that its hiring of career employees and its decisions whether and when to prosecute certain high-profile cases were affected by improper political considerations. With regard to the concerns about improper politicized hiring practices, two joint reports issued by the OIG and the Department's Office of Professional Responsibility (OPR) confirmed these allegations.

The first report, released in June 2008, examined hiring practices in the Department's Honors Program and Summer Law Intern Program. The Honors Program is a highly competitive hiring program for entry-level Department attorneys. The Summer Law Intern Program (SLIP) is a highly competitive program for paid summer internships for law students in the Department

In our report, we determined that committees used by the Department to screen applications for the two programs inappropriately used political or ideological affiliations to "deselect" candidates in 2002 and in 2006. We found that in 2002 candidates with Democratic Party and liberal affiliations apparent on their applications were deselected at a significantly higher rate than applicants with Republican Party, conservative, or neutral affiliations. This pattern continued when we compared a subset of academically highly qualified candidates. In 2006, the Screening Committee again inappropriately used political and ideological affiliations to deselect a significant number of candidates. We determined that a significantly higher percentage of the deselected Honors Program and SLIP candidates had liberal affiliations as compared to candidates with conservative affiliations. This pattern was also apparent when we compared applicants with Democratic Party affiliations versus Republican Party affiliations for both Honors Program and SLIP candidates, and the pattern persisted when we examined a subset of candidates who were highly qualified academically. We concluded that two members of the

2006 Screening Committee committed misconduct by taking political or ideological affiliations into account in deselecting candidates, in violation of Department policy and federal law.

The second report, issued in July 2008, examined the actions of staff in the Office of the Attorney General regarding allegations that they inappropriately used political or ideological affiliations in the hiring process for career Department positions. Our investigation found that Monica Goodling (the Department's former White House Liaison), Kyle Sampson (the former Chief of Staff to the Attorney General), and other staff in the Office of the Attorney General improperly considered political or ideological affiliations in screening candidates for certain career positions at the Department, in violation of federal law and Department policy.

We determined that Goodling often used political or ideological affiliations to select or reject career attorney candidates for temporary details to Department offices, which sometimes resulted in high-quality candidates for important details being rejected in favor of less-qualified candidates. For example, Goodling rejected an experienced career terrorism prosecutor for a detail to the Executive Office for U.S. Attorneys (EOUSA) to work on counterterrorism issues because the candidate's wife was active in the local Democratic Party. Instead, EOUSA had to select a more junior attorney who lacked any experience in counterterrorism issues and who EOUSA officials believed was not qualified for the position.

We also found that Goodling and Sampson violated federal law and Department policy by inappropriately considering political or ideological affiliations in evaluating and selecting candidates for immigration judge positions. Goodling screened candidates for immigration judges by using a variety of techniques for determining their political affiliations, including researching the candidates' political contributions and voter registration records, and using an Internet search string containing political terms. Moreover, this selection process caused significant delays in appointing immigration judges at a time when the immigration courts were experiencing an increased workload and a high vacancy rate.

A third report, issued in late September 2008, examined the Department's removal of nine U.S. Attorneys in 2006. The way the Department handled the removal process and the after-the-fact reasons proffered for the removals resulted in significant controversy, concerns that the removals were undertaken for improper political purposes, and allegations that the reasons proffered by the Department for the removals were not true. We therefore investigated in detail how each of the nine U.S. Attorneys was selected for removal and the process used to remove them. In addition, we examined the accuracy of the public statements and congressional testimony by Department officials justifying the removals.

Our report concluded that the process the Department used to select the U.S. Attorneys for removal was fundamentally flawed, and the oversight and implementation of the removal process by the Department's most senior leaders was significantly lacking. Our investigation also found substantial evidence that partisan political considerations did play a part in the removal of several of the U.S. Attorneys. In addition, after the removals became public, the statements and congressional testimony provided by senior Department officials about the reasons for the removals were inconsistent, misleading, or inaccurate in many respects.

The Department's removal of the U.S. Attorneys and the controversy it created severely damaged the credibility of the Department and raised doubts about the integrity of Department prosecutive decisions.

To its credit the Department – both prior to and since issuance of our reports on politicized hiring – has taken steps to address the problems we found in our reports. With regard to the hiring of career attorneys, the Department agreed to implement all of the recommendations in our June and July 2008 reports, including changing the process for selecting Honors Program candidates, removing the screening conducted by political officials on the Screening Committee, and providing written guidance on the criteria that should be applied to the hiring for career attorneys. With regard to the removal of the U.S. Attorneys, the Attorney General has appointed a special prosecutor to fully investigate remaining questions and make final decisions based on all the evidence as to whether any crime was committed relating to this matter.

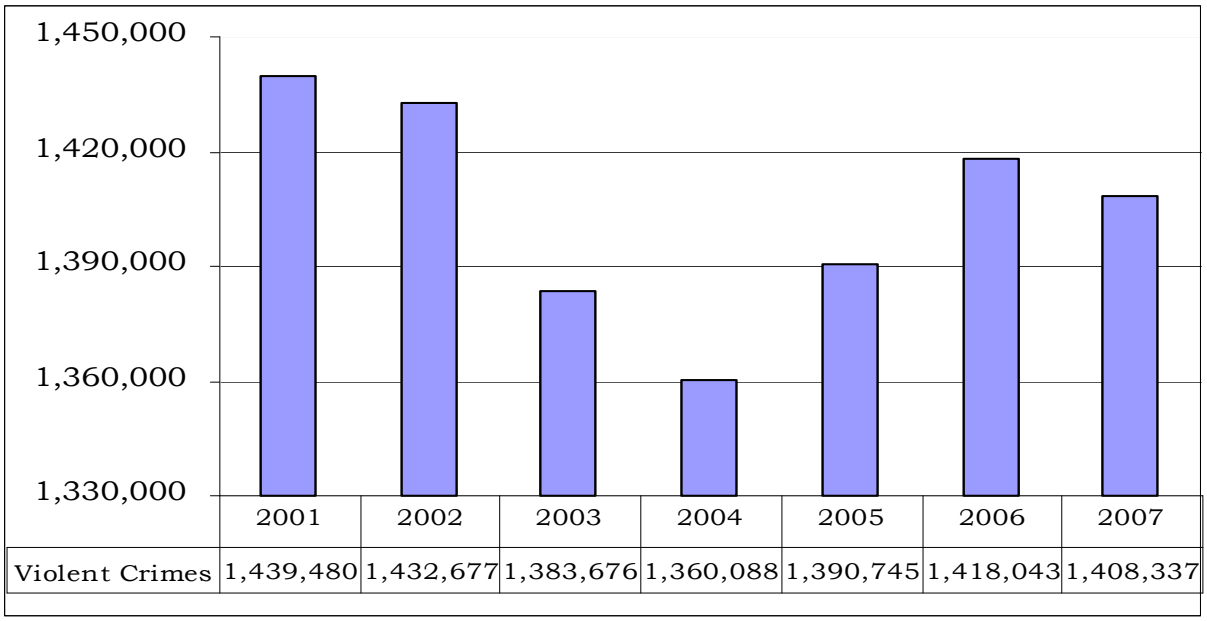
The immediate challenge for the Attorney General and the Department's leadership is to ensure that the serious problems and misconduct we found regarding politicized hiring for career positions and the dismissal of U.S. Attorneys do not recur. The Department's removal of the U.S. Attorneys and the controversy it created severely damaged the credibility of the Department and raised doubts about the integrity of Department prosecutive decisions. We believe that final resolution of the issues raised in our report can help restore confidence in the Department by fully describing the serious failures in the process used to remove the U.S. Attorneys and by providing lessons for the Department in how to avoid such failures in the future.

With regard to the upcoming change in Administrations, the Department must coordinate effectively with the Department's new leadership to accomplish an orderly and efficient transition. In addition to continuing to restore confidence in the Department over the long run, the incoming Attorney General must address in a timely way the serious challenges facing the Department, many of which are described in this document.

6. Violent Crime: The Department's Strategic Plan recognizes as priorities the need to "reduce the threat, incidence, and prevalence of violent crime" and the need to "strengthen partnerships for safer communities and enhance the Nation's capacity to prevent, solve, and control crime."

Although the number of violent crimes in 2007 decreased by 0.7 percent compared with 2006, violent crime remains a continuing challenge for the Department and the country. As shown in the chart below, in 2007 there were 467 violent crimes per 100,000 inhabitants, or about 1 violent crime per 217 people. The FBI Uniform Crime Report on trends in the number of violent crimes reported to law enforcement across the United States in 2007 shows that aggravated assault accounted for 61 percent of violent crimes, robbery 32 percent, forcible rape 6 percent, and murder 1 percent. All of these percentages remained steady between 2006 and 2007.

Chart 1 – Number of Reported Violent Crimes 2001 – 2007



	2001	2002	2003	2004	2005	2006	2007
Violent Crimes	1,439,480	1,432,677	1,383,676	1,360,088	1,390,745	1,418,043	1,408,337

While the Department's post-September 11 priorities were reordered to emphasize preventing terrorism, an ongoing challenge has been to maintain an appropriate emphasis on domestic crime. One key element of this challenge is for the Department to effectively coordinate new initiatives to address violent crime with existing operations, including among the Department's task forces and partnerships with state and local law enforcement agencies. A May 2007 OIG report found that coordination efforts among four of the Department's law enforcement components' task forces were not fully effective at preventing duplication of effort. In response to our report, the Department issued a policy requiring U.S. Attorneys to report to the Department on violent crime task force coordination efforts, on coordination problems, and on guidance or policies adopted or revised to address the problems. Also, the Department now requires components to obtain the Deputy Attorney General's approval before implementing new violent crime task forces to ensure better coordination.

As part of the Department's Project Safe Childhood initiative, the FBI operates various programs to combat crimes against children, such as child abduction and exploitation. For example, to combat the prostitution of children, the FBI's Innocence Lost National Initiative coordinates with the National Center for Missing and Exploited Children and the Department's Child Exploitation and Obscenity Section. In FY 2007 the Department's Internet Crimes Against Children program, a national network of 59 regional task forces that investigate computer-facilitated child sexual exploitation, recorded more than 2,350 arrests. The OIG is currently auditing the FBI's efforts to combat crimes against children to examine whether the FBI has effectively established a nationwide investigative response to address the sexual exploitation, abduction, and abuse of children.

Because combating violent crime depends in large part on state and local responses, the Department pursues many of its anti-crime goals through grants to support local law enforcement

violent crime reduction efforts and by sharing intelligence and law enforcement information with local law enforcement, as well as by directly investigating interstate criminal activities, often through task forces and partnerships with state and local law enforcement.

Regarding grants, in FY 2008 the Department awarded almost $2.8 billion to states and local agencies to assist with criminal justice activities, including gang reduction activities. As is discussed further in the Grant Management Challenge, proper oversight and evaluation are needed to ensure that these funds are being used for their intended purpose and that the activities they support are effective.

The OIG is reviewing the Department's implementation of the *Sex Offender Registration and Notification Act* (SORNA), which increased federal enforcement of sex offender registration requirements and penalties for sex offenders who fail to register or update their registrations. The act also designated the United States Marshals Service (USMS) as the lead agency for investigating fugitive sex offenders. We found that Department has made progress in implementing SORNA, including issuing guidelines on compliance for states; working to make state, territory, and tribal registries accessible through the Department's National Sex Offender Public Registry web portal; and expanding access to the FBI's National Crime Information Center criminal history database. Further, the USMS has increased federal investigations and arrests of fugitive sex offenders and has increased the assistance it provides to state agencies with fugitive sex offender investigations. However, we also found that the national sex offender registries are incomplete and inaccurate and are not reliable sources of information on sex offenders for law enforcement and the public.

Another OIG review is examining the operations of two organizations central to the Department's anti-gang effort – the National Gang Intelligence Center (NGIC) and the National Gang Targeting, Enforcement, and Coordination Center (GangTECC). NGIC is a multi-agency entity where intelligence analysts from federal, state, and local law enforcement can work together to develop and share gang-related information to provide a centralized intelligence resource for gang information and analytical support to law enforcement. Under GangTECC, the Department's operational components and other federal agencies coordinate to ensure that tactical and strategic intelligence is shared among law enforcement agencies. GangTECC also serves as a coordinating center for multi-jurisdictional gang investigations involving federal law enforcement agencies.

In sum, while ensuring that it meets its counterterrorism-related responsibilities, the Department must at the same time maintain its focus on its violent crime initiatives and strengthen its partnerships with state and local law enforcement.

7. Cybercrime: Cybercrime involves the use of computers to conduct criminal activity, such as fraud, identity theft, sexual exploitation of minors, and theft of intellectual property. With rapid technological advances and the widespread use of the Internet, combating cybercrime represents a continuing challenge for the Department and law enforcement nationwide.

Cybercrime poses a significant threat to U.S. national economic and security interests. While there is no single reliable measure of losses sustained by U.S. business as a result of cyber attacks, the estimated losses are staggering. For example, the FBI's 2005 Computer Crime Survey described as conservative its $67.2 billion estimate of total loss to U.S. businesses from computer attacks. The Computer Security Institute (CSI) 2007 Computer Crime and Security Survey, the successor to the joint CSI/FBI computer crime survey conducted in past years, reported that the average loss suffered by a more limited number of survey respondents more than doubled from $168,000 in 2006 to $345,000 in 2007. This indicates that the economic impact of cybercrime is significant and growing. Moreover, computers and other information technology systems have become part of our critical infrastructure, making their protection central to national security.

In recognition of the global scope and rapid growth of cybercrime, the Department participates in a working group with five other countries to share knowledge, experience, and best practices to counter the rising threat associated with computer intrusions. In addition, the FBI's Cyber Division manages the FBI's overall cybercrime program in light of the international aspects and national economic implications of cyber threats. The FBI also participates in the Internet Crime Complaint Center (IC3) to better track and refer for investigation and prosecution instances of computer crime.

Three of the Department's Criminal Division sections also play key roles in the Department's ongoing response to cybercrime: the Fraud Section leads the Department's Internet Fraud Initiative; the Child Exploitation and Obscenity Section (CEOS) coordinates efforts to prosecute Internet sex crimes against children; and the Computer Crime and Intellectual Property Section (CCIPS) focuses on electronic penetrations, data thefts, and cyber attacks on critical information systems.

The Criminal Division 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 August 2008, more than 200 specially trained Assistant U.S. Attorneys in each of the 94 U.S. Attorneys offices are investigating and prosecuting computer crime and intellectual property offenses.

The OIG's March 2008 audit of the Department's Key Indicators related to implementation of its Strategic Plan assessed the Department's response to two aspects of the challenges posed by cybercrime. We found that some of the measures used by the Department to assess its impact on cybercrime are faulty. For example, the FBI collects and counts Internet fraud complaints through the IC3 and refers them to FBI field offices and state and local law enforcement agencies. In each of the past four years, the IC3 has received and referred more than 200,000 complaints. However, we concluded that counting the number of complaints and referrals failed to measure the number of Internet fraud targets actually neutralized because there is no process or requirement for FBI field offices or state and local law enforcement agencies to report back to the IC3 whether an investigation was opened or whether any neutralization resulted from the referral. In response to our recommendation, FBI field offices are now required to report to IC3

all Internet Fraud investigations opened, including those resulting from IC3 referrals, and to provide regular progress updates on such investigations.

In that same March 2008 audit, we concluded that the FBI's key indicator for identifying the number of child pornography websites and web hosts shut down was not accurate because it used as a surrogate measure the number of subpoenas for subscriber information served on web hosting companies and Internet service providers (ISP). Counting the number of subpoenas served is not a fully accurate measure of the FBI's activities in shutting down child pornography websites and web hosts because the FBI has no direct technical role in shutting down the websites. The FBI concurred with the audit report's recommendation to revise this key indicator to more accurately measure the FBI's role and activities.

Additionally, the OIG is now reviewing the FBI's efforts to combat crimes against children. This audit includes a review of the FBI's national and international investigative response to the online sexual exploitation of children through its Innocent Images National Initiative. Our preliminary findings indicate that the FBI has appropriately focused 70 percent of its Innocent Images special agent resources on its top two priorities – enterprises and producers who sexually exploit children online. However, we identified issues with the timely processing of evidence seized from computers and other electronic devices in investigating cybercrimes against children. For example, we found a significant backlog in the FBI's examination of computer-based evidence in crimes against children cases. While the FBI submitted a proposal to the Department in March 2007 to address the backlog, this proposal has not yet been acted upon.

In sum, the Department and its components have taken action to combat the varied facets of cybercrime, but the Department must continue to respond to this growing challenge.

8. Grant Management: Concerns about the integrity of the Department's grant award process during the past year focused renewed attention on the Department's efforts to effectively manage the billions of dollars it awards in grants each year.

For at least the past 8 years, the OIG has identified grant management as a significant challenge for the Department, not only in terms of making timely awards of grant funds, but also in maintaining proper oversight over grantees to ensure the funds are used as intended.

At the request of Congress, the OIG is now reviewing whether the National Institute of Justice (NIJ) awarded its grants and contracts through a fair and open competitive process and the extent of its administrative costs. The current OIG audit will determine whether competitive NIJ grant and contract awards in the last 3 fiscal years were based on fair and open competition, whether non-competitive NIJ grant and contract awards were properly justified, and whether costs related to NIJ grants and contracts that were administrative in nature were properly identified.

In addition, we initiated an audit to evaluate OJJDP's grant making procedures. In FY 2007, Congress provided more than $100 million to OJJDP without earmarks and provided OJJDP an opportunity to solicit competitive proposals for new grant projects from the juvenile justice

community. The ongoing OIG audit will examine how OJJDP announces competitive award programs, reviews applications for funding, and selects awardees.

During the past year the OIG continued to assess OJP's role in administering the external investigation certification requirement for the Paul Coverdell Forensic Science Improvement Grants Program. Pursuant to this requirement, Coverdell grant applicants must certify that a government entity exists and an appropriate process is in place to conduct independent external investigations into allegations of serious negligence or misconduct – such as false testimony by some forensic laboratory staff – that substantially affect the integrity of forensic results.

Our January 2008 report found continued deficiencies in OJP's administration of the Coverdell program. We found that although OJP had complied with the minimum terms of the statute to obtain certifications from grant applicants, OJP was still not effectively administering the external investigation certification requirement. In response to our report, OJP agreed to make changes in the FY 2009 Coverdell Program announcement actions that will strengthen the certification process and improve OJP's administration and monitoring of this grant program.

In July 2008, the OIG issued a report on OJP's Human Trafficking grant program that seeks to assist human trafficking victims and fund task forces to identify and rescue victims. Our audit found problems with the design and management of the program, with grantees' compliance with essential grant requirements, and with OJP's system for monitoring human trafficking service providers and task forces.

In particular, we found that the Department's award process resulted in a wide variation in funds awarded compared to the number of victims anticipated to be served. For example, one service provider received $1,896,535 to supply services to an estimated 100 victims over the 3-year agreement period, or $18,965 per estimated victim. Another provider received $490,829 to service an estimated 100 victims over the 3-year agreement period, or $4,908 per estimated victim. For the 19 agreements we tested, the amount awarded per anticipated victim ranged from a high of $33,333 to a low of $2,500. In addition, we found that the service providers and task forces significantly overstated the number of victims they served, and the Department included this inaccurate information in its annual reports to Congress. We made 15 recommendations to strengthen management OJP's human trafficking grant programs, all of which OJP agreed to implement.

Also in 2008, the OIG reviewed 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. Our audit found weaknesses in monitoring and oversight of SWBPI funds. Specifically, OJP did not require applicants to provide documentation supporting reimbursement requests and does not review applications for allowability and accuracy. We also found that SWBPI reimbursements were not linked to actual costs incurred by the jurisdictions to prosecute federally declined-referred criminal cases. Further, OJP had not taken action to identify potential duplicate funding between the SWBPI program and other federally funded prosecution and pre-trial detention programs.

As part of the review, we conducted audits of seven SWBPI recipients to determine if SWBPI reimbursements were allowable and supported. Our audits identified unallowable and unsupported SWBPI reimbursements of $15.57 million of the $55.11 million awarded in those seven grants, or 28 percent of the total reimbursements.

Other recent OIG audits of grant recipients demonstrated a continuing need for improved grant oversight by the Department. For example, in March 2008 we issued an audit on a $3.16 million Bureau of Justice Assistance (BJA) grant administered by the National Training and Information Center (NTIC) in Chicago, Illinois, to provide training, technical assistance, and funding to community-based organizations. More than half the grant funds were awarded to subgrantees who were supposedly selected based on their ability to run a successful community program. However, our review revealed that the majority of subgrantees were selected instead based on their connections to influential lawmakers. In addition, we found inadequate controls over expenditures, unallowable personnel costs, improper and unallowable non-personnel costs, and contractor irregularities. In the end, we questioned the entire $3.16 million grant and made 37 recommendations to OJP to address the deficiencies we identified during our audit. OJP agreed with our recommendations and suspended funding to NTIC. At the same time, the OIG's Investigations Division initiated a criminal investigation related to this grant and, as a result, the NTIC Executive Director pled guilty to misuse of federal grant funds.

The OIG's Investigations Division successfully concluded several other grant fraud investigations this year. For example, in February 2008, following a 3-week trial, James Hayes, the former mayor of Fairbanks, Alaska, was convicted after trial in the District of Alaska on 16 counts of theft of government funds, conspiracy, money laundering, and submitting false tax returns. Hayes and his wife were previously charged in a 97-count indictment with theft of $450,000 of federal grant funds, conspiracy, filing false tax returns and money laundering. The investigation developed evidence that Hayes and his wife misappropriated Department grant funds designated to operate a non-profit organization called Love Social Services Center by using those funds for personal use and the construction of their church. James Hayes was sentenced to 66 months' incarceration, while his wife was sentenced to 3 years' incarceration pursuant to her guilty plea.

During the past year OJP has made some progress in staffing its Office of Audit, Assessment, and Management (OAAM), a unit intended to improve internal controls and streamline and standardize grant management policies and procedures across OJP. While OAAM had a significant number of vacancies heading into FY 2008, during the past year it filled all but one of those open positions and in September 2008 hired its first permanent director.

Finally, the OIG continues to participate in the National Procurement Fraud Task Force during the past year and chairs the task force's Grant Fraud Committee.

In sum, management and oversight of the billions of dollars in Department grants awarded annually remains a top Department management challenge.

9. Detention and Incarceration: The Department's ability to safely and economically manage increasing federal detainee and inmate populations presents a critical management challenge, particularly in light of overcrowding, lack of economical alternative detention space, stresses on prison staffing, and the rising cost of inmate health care.

Between October 2003 and August 2008, the federal inmate population rose from 172,499 to 201,214 inmates, an increase of approximately 17 percent. While the Federal Bureau of Prison's (BOP) total budget during that same period increased by about 20 percent (including one time reprogramming and emergency supplemental funds), the BOP's budget has not kept pace with the eight-fold growth in the BOP inmate population over the past 25 years.

The Department continues to report prison overcrowding as a material weakness in its annual performance and accountability reports, and the Department's stated goal is to reduce crowding in federal prisons to 28 percent by 2012. To that end, the BOP has expanded existing facilities, acquired surplus properties for conversion to correctional facilities, built new facilities, and housed male low-security special population inmates in private contract and state and local facilities. Notwithstanding these steps, the BOP projects the overcrowding rate to increase to 36 percent by the end of FY 2008 and to 37 percent by the end of FY 2009.

BOP officials believe that expanding existing institutions is the least expensive way to accommodate more federal inmates, and the BOP has built additional inmate housing at facilities where the infrastructure can absorb population increases. However, the infrastructure at many institutions has already reached its limit. Approximately one-third of BOP's 114 institutions are more than 50 years old and renovation or expansion of these older facilities is not economically feasible because their infrastructure (including basic utilities) is designed for significantly smaller inmate populations. Further, according to BOP officials, overcrowding at all medium and high security facilities has accelerated the facilities' deterioration and need for renovations.

Construction of new institutions has also presented difficult challenges. A May 2008 review by the Government Accountability Office (GAO) examined construction estimates for three new BOP facilities and found that delays in beginning construction and disruptions in construction because of funding issues contributed significantly to these projects costing 62 percent more than budgeted.

In addition, an October 2007 GAO report found that the cost of contracting with non-BOP facilities to confine male low-security special population federal inmates nearly tripled from about $250 million in FY 1996 to about $700 million in FY 2006. GAO recommended that the BOP examine whether building new BOP facilities for low-security inmates would be more cost-effective than continuing to rent confinement space for this rapidly increasing population. In response to the GAO report, BOP concluded that its competitive contracts for space provided a more flexible and quicker option for adding capacity compared to new construction. During FY 2009, however, the OIG plans to audit BOP's contracting for confinement space to determine whether the contracts result in the best value for the money spent.

The need to address overcrowding within its budget has also forced BOP to cut costs elsewhere in the federal prison system. To that end, BOP has streamlined and centralized many of its

administrative functions. In addition, it has cut costs in its handling of minimum security inmates by closing several stand-alone prison camps, transferring inmates to camps associated with other facilities, and moving inmates with critical medical needs to dedicated BOP medical centers. These steps have resulted in the elimination of 2,300 BOP positions.

In addition to the challenge that overcrowding presents in terms of confinement space, it can also affect the safety and security of the federal prison system. In recent years, there have been several significant incidents of inmate violence at BOP institutions. In response to some of these incidents, BOP staff members have claimed that staffing shortages and prison overcrowding, complicated by gang rivalries, led to the violence. According to BOP officials, as of October 9, 2008, 13 percent of its staff positions – including more than 8 percent of Corrections Officer positions – are unfilled at BOP's 114 institutions.

The OIG currently has three reviews underway that examine various aspects of BOP programs. In our review of the operations of Federal Prison Industries, Inc., we are investigating allegations that the BOP failed to adequately address allegations that workers and inmates at several BOP institutions were exposed to unsafe levels of lead, cadmium, and other hazardous materials in computer recycling plants. In an audit of the BOP's Witness Security Program (WITSEC), we are examining controls in place over physical security, housing assignments, prisoner transport, and access to information in database systems about federal inmates who participate in WITSEC for their safety in connection with federal prosecutions involving organized crime, drug trafficking, and terrorism. A third ongoing OIG review is assessing the BOP's efforts to deter sexual abuse of inmates by prison staff.

In addition to the challenges relating to the BOP's housing of federal inmates, the Department must also provide adequate and economical housing for the increasing number of federal detainees taken into custody by the United States Marshal Service (USMS). Approximately 59,000 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 2008 totaled more than $1.2 billion.

The USMS houses about 20 percent of its federal detainees in BOP facilities. The remaining detainees are placed in space leased from state and local governments (66 percent) and private correctional facilities (13 percent). The USMS maintains contracts, known as Intergovernmental Agreements (IGA), with about 1,800 state and local facilities to house these detainees. In OIG audits of Department IGAs over the years, we have found problems with the manner in which the detainee-per-day charges are determined and with the Department's monitoring of the charges. In November 2007, the OFDT implemented a pricing model, referred to as eIGA, in an attempt to ensure that the rates paid by the federal government are fair and reasonable. The OFDT is attempting to refine the eIGA so that operating cost information gathered from detention facilities is converted into an estimated, reasonable per diem rate that contracting officials can use as a baseline in negotiating the IGA rates.

Both the BOP and the USMS also face challenges in containing health care costs and providing quality health care for inmates and detainees. From FY 2000 through 2007, the BOP spent about

$4.7 billion for inmate health care. In a February 2008 audit, the OIG examined the growth of inmate health care costs over the past 7 years and found that the BOP has kept this growth at a reasonable level compared with national health care cost data reported by the Departments of Health and Human Services and Labor. Yet, while the BOP has implemented cost containment strategies to provide health care to inmates in an effective and efficient manner, we noted that it could possibly further reduce costs. For example, we found that some BOP institutions fail to review and verify medical bills of health care providers.

In sum, addressing the varied facets of the detention and incarceration of federal detainees and inmates presents ongoing challenges for the Department.

10. Financial Management and Systems: The Department has continued to make progress in addressing the major problems identified in the OIG's annual financial statement audits. However, while the Department and its components deserve significant credit for improvements in its financial management systems, the Department still lacks a unified financial management system 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 FY 2008, the Department again earned an unqualified opinion and improved its financial reporting. For the second straight year, the financial statement auditors did not identify any material weaknesses at the consolidated level. Additionally, Department components reduced component material weaknesses from four in FY 2007 to one in FY 2008. Similar to past years, however, much of this success was achieved through heavy reliance on contractor assistance, manual processes, and protracted reconciliations. We remain concerned about the sustainability of these ad hoc and costly manual efforts.

In recent years, we have seen a key improvement in the Department's financial statement audits with the expanded involvement of Department managers in issuing guidance and providing greater assistance with component audits and corrective action plans. The Department has also continued to expand its internal control review process to include assessments of the components' information systems control environment, improper payment improvement program, and oversight of purchase card usage. These actions have enabled the Department to monitor the components' corrective action plans more timely and, when necessary, provide additional resources to correct internal control weaknesses.

Yet, none of the Department's six major accounting systems currently 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. As a result, many financial 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. We support these efforts and believe the UFMS can help eliminate the weaknesses in the Department's disparate financial management systems.

The Department's efforts over the past several years to implement the UFMS to replace the six major accounting systems currently used throughout the Department have been subject to fits and starts, primarily because of problems obtaining sufficient funding for the UFMS, staff turnover, and other competing priorities that have caused delays in implementing the UFMS.

Four years have passed since the Department selected a vendor for the unified system, and full implementation of UFMS at the first component, the Drug Enforcement Administration, is not scheduled to begin until FY 2009, more than 1 year behind schedule. Furthermore, implementation of the UFMS is not projected to be completed in all Department components until FY 2013 at the earliest. Until that time, Department-wide accounting information will 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.

Several recently issued OIG audits have also highlighted other financial management concerns beyond financial statements. For example, the FBI uses confidential funds to conceal its identity from criminals, vendors, or the public during FBI undercover activities. A January 2008 OIG audit of the FBI's management of these confidential case funds found that the FBI lacked an adequate financial system necessary to manage these funds effectively. Consequently, FBI employees developed various "work-arounds" to the system in an effort to track confidential case fund requests made by FBI special agents operating in undercover capacities, but these efforts were not completely successful. Our review found that the sheer volume of bills, coupled with the inconsistent way various FBI field offices handle confidential case funds, resulted in the FBI routinely paying covert telecommunication costs late, which sometimes resulted in telecommunication carriers terminating FBI telephone lines for non-payment in important cases.

In sum, the Department continues to show improvement in its overall financial management, with another year of positive financial statement audit results. However, the lack of a single integrated financial management system to replace the disparate financial systems used by Department components will continue to handicap future progress. The key to improving the Department's financial management rests on the timely implementation of the Unified Financial Management System throughout the Department.