OIG Top Management and Performance Challenges in the Department of Justice

November 9, 2010

MEMORANDUM FOR THE ATTORNEY GENERAL

THE ACTING DEPUTY ATTORNEY GENERAL

FROM: GLENN A. FINE
INSPECTOR GENERAL

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

Attached to this memorandum is the Office of the Inspector General's (OIG) 2010 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.

We hope this document will assist Department managers in addressing the top management and performance challenges facing the Department. We look forward to continuing to work with the Department to respond to these important issues.

Attachment

This page intentionally left blank.

Top Management and Performance Challenges in the Department of Justice – 2010

1. Counterterrorism: Counterterrorism is the highest priority of the Department of Justice (Department or DOJ), and the Office of the Inspector General (OIG) has consistently identified it as a top management challenge facing the Department. Various public examples of terrorism attempts, including the attempt on December 25, 2009, to detonate an explosive device on board a flight from Amsterdam to Detroit and the attempt on May 1, 2010, to detonate a bomb in Times Square in New York City, illustrate the continuing threat of terrorism. While the Department has made progress in combating terrorism, we believe the Department continues to face significant challenges in this area.

To address the threat of terrorism, the Department has undergone transformational changes in its counterterrorism efforts, such as the creation of the National Security Division in 2006 to consolidate the Department's primary national security operations. In addition, the Department's law enforcement components, including the Federal Bureau of Investigation (FBI), the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the Drug Enforcement Administration (DEA), and the United States Marshals Service (USMS), have undergone structural changes since 2001 to allow them to better address terrorism. Yet, the Department must ensure that it and its components are effectively sharing that information to disrupt attacks and to respond effectively to acts of terrorism.

The Department also must be prepared to ensure public safety in the event of a terrorist act. In a recent review, the OIG concluded that the Department needs to improve its response preparedness. The OIG's June 2010 report on the readiness of the Department and its components to respond to a potential weapons of mass destruction (WMD) incident found that the FBI had taken appropriate steps to prepare to respond to a WMD attack, such as establishing WMD response plans, providing WMD training to FBI staff on responding to a WMD incident, and regularly conducting and participating in WMD response exercises. However, we also found that the Department as a whole was not fully prepared to provide a coordinated response to a potential WMD attack and had not implemented adequate WMD response plans.

In particular, the Department's management of plans for responding to a WMD attack was uncoordinated and fragmented, with no entity or individual assigned responsibility for central oversight of WMD response activities throughout the Department. We also determined that Department-level critical incident response policies and plans had not been fully implemented, were not in compliance with national policies, were outdated, and did not specifically address the appropriate response to a WMD attack. In addition, we found inadequate efforts among Department components to coordinate a response to a WMD incident. No Department law enforcement component, other than the FBI, had specific WMD operational response plans. Moreover, other than the FBI, Department components provided little to no training for responding to a WMD incident and rarely participated in WMD exercises.

In addition, while the Department had designated ATF as the lead agency to coordinate the use of federal law enforcement resources to maintain public safety and security if local and state resources are overwhelmed during a WMD incident, ATF had not adequately prepared for this role. When we specifically examined the readiness of Department components' field offices in the Washington National Capital Region (NCR) to respond in a coordinated way to a WMD incident, we found that outside of special events, only the FBI had conducted WMD-specific planning or training in the NCR.

The Department responded constructively to our report, assigning the Associate Deputy Attorney General for National Security the responsibility for coordinating all Department policies associated with continuity of operations, continuity of government, and emergency response at the scene of an incident. The Department also established a committee to develop policy, training, and strategies to ensure that the Department as a whole is ready to respond to a WMD incident. While the Department has begun to address the deficiencies we identified, we will continue to assess the progress of the Department in this area.

Another example of insufficient counterterrorism coordination among Department components relates to the FBI and ATF response to explosives incidents. Federal law gives the FBI and ATF concurrent jurisdiction over most federal explosives incidents. In an October 2009 review, we determined that the FBI and ATF had developed separate and often conflicting approaches to explosives investigations and explosives-related activities such as training, information sharing, and forensic analysis. These conflicts resulted in unnecessary competition and duplication of efforts and also could result in problematic responses to explosions, including terrorist incidents. In response to our report, in August 2010 the Acting Deputy Attorney General issued a new protocol designed to improve coordination between the FBI and ATF. The protocol described factors that are strong indicators of a nexus to terrorism – such as the use of a chemical, biological, radiological, or nuclear agent or an attack on a government building, mass transit, or a power plant – and assigned lead-agency jurisdiction based on those factors to the FBI. The new protocol gave ATF lead jurisdiction to investigate explosives incidents that do not involve a credible terrorism nexus and which are not governed by agreements between ATF and FBI either locally or at the headquarters. The Acting Deputy Attorney General also directed ATF and the FBI to develop a joint plan for consolidated explosives training and to convene a board to discuss how laboratory resources and training could be better coordinated and integrated.

We believe these actions are positive steps that can improve coordination between the FBI and ATF. However, the Department needs to ensure that its protocols are workable and are enforced, and that the FBI and ATF consistently coordinate and cooperate in explosives investigations.

Another important Department counterterrorism responsibility involves the management of the consolidated terrorist watchlist. This watchlist is used by frontline government screening personnel to determine how to respond when a known or suspected terrorist requests entry into the United States. In May 2009 the OIG issued an audit examining the FBI's practices for making nominations to the consolidated terrorist watchlist. The audit concluded that the FBI did not consistently nominate known or suspected terrorists to the terrorist watchlist in a timely manner or in accordance with FBI policy, and the FBI also did not update or remove watchlist records as required. Since we issued our report, the FBI has reported that it has improved the

timeliness of its nomination activities and has increased its monitoring of field office submissions. The OIG recently initiated a new review of the FBI's management of the watchlist to assess the progress in this area.

The Department also seeks to disrupt terrorist acts by attacking terrorists' financing. The OIG is currently reviewing the FBI's and the National Security Division's (NSD) efforts to identify, investigate, and prosecute terrorist-related financing activities. Our audit is also reviewing how the FBI and NSD coordinate efforts throughout the law enforcement community to combat terrorist-financing operations.

In addition to improving information sharing and coordination, the Department also should regularly evaluate the balance of resources devoted to counterterrorism and traditional law enforcement activities. In April 2010, we issued a report that examined the process by which the FBI assigns its personnel resources, including how the FBI utilizes agents and intelligence analysts on counterterrorism matters and other investigative areas such as violent crime, white collar crime, and cyber crime. Our review also detailed changes in the FBI's caseload by investigative area.

We determined that in fiscal year (FY) 2009, 26 percent of FBI agents were assigned to counterterrorism matters, which was double the percentage of agents assigned to such matters in FY 2001. We also found that the FBI generally used field agents in line with the level it allocated for counterterrorism activities in FY 2009. In addition, we found that the FBI has improved its ability to monitor and evaluate its allocation and utilization of personnel resources by establishing a Resource Planning Office and by developing an extensive management information system. In addition, the FBI has established various resource management initiatives to oversee the allocation and utilization of personnel resources.

Our report recommended that, to further improve the allocation of resources, including counterterrorism resources, the FBI should develop a more sophisticated resource allocation methodology and regularly examine personnel resource utilization associated with division-specific priorities. In recent correspondence, the FBI stated that it has implemented such a resource allocation methodology and is taking action to implement the rest of our recommendations. We believe that these actions can improve the FBI's management of its personnel resources based on a risk-based analysis of threats and FBI priorities.

The Department is also faced with the challenge of hiring employees with specialized skills that are essential to its counterterrorism efforts, such as employees with foreign language capabilities or expertise in information technology. In a follow-up review we conducted of the FBI's Foreign Language Translation Program, we reported that the FBI continued to have significant amounts of unreviewed foreign language materials in counterterrorism and counterintelligence, the FBI's highest priority investigative areas. The FBI also continued to fall short in meeting its linguist hiring goals, resulting in a decrease in the number of FBI linguists at the same time the FBI has increased the amount of material it collects for translation. Without sufficient linguist resources, the FBI will not be able to review all the high-priority material it collects, increasing the risk that the FBI will not detect information in its possession that is important to its counterterrorism and counterintelligence efforts. In response to our report, the FBI stated that it

is in the process of accelerating timeframes for converting part-time contract linguists to full-time FBI linguist positions and is implementing plans to add Investigative Analyst Consultants to assist in reducing timeframes for security clearance adjudications.

In sum, the Department must continue to improve information sharing and coordination in its counterterrorism efforts, and we believe that counterterrorism remains a critical challenge for the Department.

2. Restoring Confidence in the Department of Justice: We first identified this as a top management challenge after the controversy concerning the Department's firing of U.S. Attorneys and the politicized hiring of certain career Department employees. We believe the Department has taken aggressive steps to respond to these issues. However, other issues of concern persist, such as allegations of prosecutorial misconduct and the Department's ability to address these allegations in a timely and transparent manner. We believe that restoring confidence in the Department remains a top management challenge.

In 2008 and 2009 the OIG and the Department's Office of Professional Responsibility (OPR) issued three joint reports that substantiated serious allegations of improper politicization in hiring for career attorney positions in the Department's Honors Program and Summer Law Intern Program, for other career positions, and in the Civil Rights Division. Another joint OIG/OPR report concluded that partisan political considerations played a part in the Department's removal of U.S. Attorneys in 2006.

To correct problems we found in these reviews, the Department has taken important steps, such as returning the responsibility for hiring career employees from politically appointed officials to career employees and developing new training that stresses that the process for hiring career employees must be merit based. The Department also invited individuals who had applied to the Department's Honors Program in 2006 and who may have been excluded for reasons of political affiliation to reapply. The Department offered positions to 17 of the 54 attorneys who chose to reapply and interview for the positions.

In addition, the former Attorney General appointed a special counsel to investigate whether any crime was committed related to removal of the U.S. Attorneys. That investigation was concluded in July 2010 with a determination by the special counsel that the evidence "did not demonstrate any prosecutable criminal offense" was committed with regard to the removal of U.S. Attorney David Iglesias of New Mexico and that the evidence did not justify broadening the scope of the investigation beyond the removal of Iglesias. The special counsel also concluded "that DOJ leadership never determined whether the complaints about Mr. Iglesias were legitimate and that the fact that the investigation of the complaints about Iglesias's performance never occurred bespeaks undue sensitivity to politics on the part of DOJ officials who should answer not to partisan politics but to principles of fairness and justice."

Although the Department has addressed most of the recommendations in the OIG/OPR reports, it still has not fully addressed one recommendation. We found that the Department had considered certain career attorneys' political or ideological affiliations when deciding whether to approve temporary details of these attorneys to certain high-level Department positions. We

recommended that the Department clarify the circumstances under which political or ideological considerations may be considered when assessing career candidates for details to various Department positions. The Department agreed with the recommendation but has not yet implemented corrective action.

The Department has been subject to significant criticism for some of its prosecutorial actions, including allegations of misconduct in the prosecution of former Alaska Senator Ted Stevens. Articles have also focused attention on other allegations of misconduct by federal prosecutors and the process by which the Department investigates such allegations. For example, a recent study released in October 2010 by the Northern California Innocence Project found 64 cases in California where courts determined there was prosecutorial misconduct by federal attorneys. In 38 of those cases, the federal courts found the misconduct resulted in harmful error and either set aside the conviction or sentence, declared a mistrial, or barred the introduction of certain evidence.

The Department has taken a variety of actions to address the issue of prosecutorial misconduct. For example, in January 2010 the Department issued a document entitled Guidance for Prosecutors Regarding Criminal Discovery, which provides requirements for prosecutors' discovery obligations, such as what material must be reviewed, how the review should be conducted, and how disclosure should be made. The Department also appointed a National Coordinator of Criminal Discovery Initiatives to oversee training for prosecutors, supervise the creation of centralized resource materials, and oversee other projects relating to criminal prosecutions. All Department prosecutors are now required to annually complete 2 hours of training on the government's criminal disclosure obligations and policies, and new prosecutors are required to complete more extensive training on this topic within their first 12 months of employment. In addition, the Department has designated "discovery experts" in all 94 United States Attorneys' Offices and in the Department's criminal litigating components. The Department also plans to reconvene a Computer Forensics Working Group to address the problem of properly cataloging electronically stored information recovered as part of federal investigations. These initiatives demonstrate commitment by the Department to improving training for prosecutors and for seeking to prevent prosecutorial misconduct.

However, we believe the Department faces additional challenges in ensuring that it has an adequate process to investigate and hold accountable any Department attorneys who commit professional misconduct. The transparency, effectiveness, and timeliness of the Department's internal process to address allegations of prosecutorial misconduct have been questioned, and we believe the Department should take action to improve the transparency of that process. For example, OPR, the internal entity that investigates allegations of prosecutorial misconduct by Department attorneys, has taken steps during the past 2 years to address the backlog in its annual reports and to more promptly post its annual reports containing summaries of its investigations of allegations of prosecutorial misconduct. However, these reports provide only limited details on the cases and the basis of OPR's conclusions. The Acting Deputy Attorney General recently stated that the Attorney General has directed the Department "to work on finding ways to make more information available to the public about these matters." We believe this is one important step. However, we believe that the timeliness and transparency of the Department's internal

processes for addressing allegations of prosecutorial misconduct need improvement to increase public confidence in the Department's ability to address such allegations.

Allegations have also arisen regarding the enforcement of federal voting rights law by the Voting Section of the Civil Rights Division. The OIG recently initiated a review of the enforcement of civil rights laws by the Voting Section that will examine the types of cases brought by the Voting Section over time, any changes in Voting Section enforcement policies or procedures, whether the Voting Section has enforced the civil rights laws in a non-discriminatory manner, and whether any Voting Section employees have been harassed for participating in the investigation or prosecution of particular matters.

The actions of the Department's law enforcement components can also affect the public's confidence in Department operations. For example, the Department must strive to ensure that it abides by the Attorney General's Guidelines for conducting investigations and does not improperly infringe on First Amendment rights in its investigations. In September 2010 the OIG issued a report concerning allegations that the FBI had targeted certain domestic advocacy groups for scrutiny based upon their exercise of rights guaranteed under the First Amendment to the United States Constitution. In this review, we examined whether the FBI complied with the Attorney General's Guidelines in classifying and conducting certain investigations. Our review did not find that the FBI had targeted these groups for investigation on the basis of their First Amendment activities, but we concluded that the factual basis for opening some of the investigations of individuals affiliated with the groups was factually weak, that the FBI extended the duration of investigations in some cases involving advocacy groups or their members without adequate basis, and that in a few instances the FBI improperly retained information about the groups in its files. Our findings about this report are discussed in more detail in our discussion of the Department's challenge in protecting civil rights and liberties.

In September 2010 we also issued a report which found that a significant number of FBI employees had cheated on the FBI exam regarding the Domestic Investigations and Operations Guide (DIOG). The DIOG implements the Attorney General's Consolidated Guidelines for FBI Domestic Operations, which were issued in 2007 and replaced several older sets of guidelines that separately addressed the requirements FBI agents must follow in criminal investigations, national security investigations, and foreign intelligence collection. When the DIOG was implemented, the FBI assured Congress that the new guidelines "take seriously the need to ensure compliance and provide for meaningful oversight to protect privacy rights and civil liberties" and that the FBI would ensure that the FBI complied with the new guidelines. We credited the FBI for implementing comprehensive training on the DIOG and for requiring employees to take and pass a computerized 51-question exam concerning this guide. However, in our limited investigation of four FBI field offices, we found that a significant number of FBI employees had engaged in some form of cheating or improper conduct on the DIOG exam, some in clear violation of FBI directives regarding the exam. For example, some FBI employees consulted with others while taking the exam when that was specifically forbidden by the test-taking protocols. Others used or distributed answer sheets or study guides that essentially provided the answers to the test. A few exploited a programming flaw to reveal the answers to the exam. Almost all of those who cheated falsely certified on the final question of the exam that they had not consulted with others. We recommended that the FBI take action regarding those

who cheated on the DIOG exam, consider other appropriate steps to determine whether other test takers engaged in similar inappropriate conduct, and also conduct a new exam on the revised DIOG. We are awaiting the FBI's response to these recommendations, which we believe can restore confidence that all FBI agents recognize the critical importance of complying with the Attorney General's Guidelines.

In sum, the Department should continue to focus attention on meeting the challenge of restoring confidence in the Department.

3. Law Enforcement Issues Along the Southwest Border: Organized criminal activities along the 2,000-mile U.S. border with Mexico present stark challenges for the Department. According to the Department's 2010 National Drug Threat Assessment, most of the illicit drugs in the United States and thousands of illegal immigrants are smuggled across the border from Mexico by crime cartels. Criminal activity also occurs in the other direction across the border, with firearms and currency smuggled from the United States into Mexico. This year we have added law enforcement issues along the Southwest Border as one of the top management challenges for the Department.

To combat violent crime, gun smuggling, drug trafficking, and illegal immigration along the Southwest Border, the Department created the Southwest Border Enforcement Initiative, which seeks to promote cooperation and enhanced intelligence and enforcement activities to attack major Mexican-based trafficking organizations on both sides of the border. The initiative is a cooperative effort among the Department's law enforcement components and United States Attorneys' Offices, the Department of Homeland Security, and many state and local law enforcement agencies.

ATF's Project Gunrunner is a key component of the Southwest Border Enforcement Initiative. Project Gunrunner is intended to reduce cross-border drug and firearms trafficking and the high level of violence associated with these activities on both sides of the border. An OIG review of Project Gunrunner found that an increase in ATF's program activities related to firearms trafficking from the United States to Mexico, but we also found that significant weaknesses in Project Gunrunner implementation undermined its effectiveness. For example, our review found poor coordination and collaboration between ATF and other Department components, and between ATF and units of the Mexican government. In addition, ATF does not systematically and consistently exchange intelligence with its Mexican agency contacts and some U.S. partner agencies. Some ATF field agents reported that they do not find investigative leads provided to them by ATF's Field Intelligence Groups to be timely and usable. Intelligence personnel in ATF's Southwest Border field divisions also do not routinely share firearms trafficking intelligence with each other. Moreover, ATF's focus remains largely on inspections of gun dealers and investigations of straw purchasers, rather than on higher-level traffickers, smugglers, and the ultimate recipients of the trafficked guns. ATF also is not using intelligence effectively to identify and target firearms trafficking organizations operating along the Southwest Border and in Mexico.

In September 2010, after we had provided our draft report to ATF, ATF circulated a revised strategy for combating firearms trafficking to Mexico and related violence. ATF's new strategy

includes 13 key elements, such as closer coordination with other law enforcement agencies, particularly related to intelligence on drug cartels; the need to improve intelligence collection, sharing, and analysis and the prioritization of leads; improved coordination with Southwest border field divisions and ATF's Mexico Country Office, including the use of Border Liaison Officers; focusing investigations on complex conspiracy cases and entire trafficking rings; greater use of the Department's Organized Crime Drug Enforcement Task Force Program; and improved investigative coordination and intelligence sharing with Mexican law enforcement, including on gun tracing. We believe ATF's strategy can address many of the weaknesses identified in our review, but development of an implementation plan – with defined goals, specific actions, and resources – is essential to the success of this new strategy.

The OIG's report on the El Paso Intelligence Center (EPIC), a multi-agency intelligence center funded primarily by the DEA, also identified improvements that are needed in intelligence relating to Southwest Border drug smuggling and associated violence. We found that EPIC's partner agencies and users regard EPIC's products and services as valuable and useful, but we identified weaknesses that have hindered EPIC's effectiveness. For example, EPIC did not analyze some information that it alone collected regarding drug seizures, fraudulently used documents, and activities of drug traffickers. As a result, EPIC was likely overlooking drug trafficking trends and patterns that could assist interdiction investigations and operations. In addition, EPIC's coordination with federal and state intelligence organizations across the country was inconsistent, and federal agencies' requests for information from EPIC's databases have been declining since 2005 at the same time the Department's focus on trafficking and associated violence on the Southwest border was increasing.

In response to the OIG's recommendations regarding EPIC, the DEA reported it has taken steps to improve EPIC's systems for sharing information with federal, state, and local law enforcement users, and that EPIC is improving its capability to use seizure information to better identify vulnerabilities along the Southwest Border. Also, according to the DEA, EPIC will provide better access to its fraudulent documents database to authorized law enforcement agencies, including the Department of Homeland Security's Immigration and Customs Enforcement, and EPIC is incorporating performance metrics in its strategic plan.

In addition to addressing violent crime and drug trafficking problems, the Department also plays a key role in immigration policy and enforcement along the Southwest Border. The Department's Executive Office for Immigration Review is responsible for operating 59 immigration courts. In our 2008 report on allegations of politicized hiring of immigration judges, we noted that the hiring deficiencies contributed to the increasing workload of immigration judges. The backlog of immigration cases has continued to grow due to an increasing caseload and unfilled vacancies on the immigration court. We are now conducting a review that is examining the operation of the immigration courts, the backlog in immigration cases, and other issues that affect the Department's enforcement of immigration laws.

In sum, while the Department has increased its efforts to address violent crime and illegal immigration along the Southwest Border, recent OIG reviews have highlighted the need for stronger coordination among the Department's components and between the Department and

other agencies. We believe that the difficult issues confronting law enforcement agencies along the Southwest Border make this a top management challenge for the Department.

4. Civil Rights and Civil Liberties: At the same time that the Department is pursuing its counterterrorism and law enforcement responsibilities, the Department must also seek to protect civil rights and civil liberties. As Director FBI Mueller recently stated:

> If we safeguard our civil liberties, but leave our country vulnerable to a terrorist attack, we have lost. If we protect America from terrorism, but sacrifice civil liberties, we have also lost. We must work to strike that balance, every day, in every case.

Several of our recent reviews demonstrate the challenges the Department faces in pursuing this balance. For example, as noted above in the challenge on restoring confidence in the Department, in September 2010 we issued a report concerning allegations that the FBI targeted certain domestic advocacy groups for scrutiny based upon their exercise of rights guaranteed under the First Amendment to the United States Constitution. The OIG review examined FBI activities from 2001 through 2006 related to domestic advocacy groups such as the Thomas Merton Center, Greenpeace, People for the Ethical Treatment of Animals, and the Catholic Worker. Our review did not find that the FBI had targeted any of the groups for investigation on the basis of their First Amendment activities. However, we concluded that the FBI did not always act consistently with its policy requiring "strict compliance" with the Attorney General's Guidelines in certain cases implicating First Amendment rights. We found that the factual basis for opening some of the investigations of individuals affiliated with the groups was weak, that the FBI extended the duration of some investigations involving advocacy groups or their members without adequate basis, and that in a few instances the FBI improperly retained information about the groups in its files. The FBI also classified some investigations relating to nonviolent civil disobedience under its "Acts of Terrorism" classification, which resulted in the watchlisting of subjects during the pendency of the investigation.

Our report recommended that the FBI should specify the potential violation of a specific federal criminal statute as part of documenting the basis for opening a preliminary or full investigation in cases involving investigation of advocacy groups or their members for activities connected to the exercise of their First Amendment rights. We also recommended that the Department and the FBI consider whether the current Attorney General's Guidelines and FBI policies should be modified to reinstate the prohibition on retaining information from public events that is not related to potential criminal or terrorist activity. In addition, we recommended that the FBI and the Department provide further guidance on when cases involving First Amendment issues should be classified as Acts of Terrorism matters and when they should not. The FBI stated that it concurred with the recommendations in our report, and we believe the FBI should take prompt action to ensure that these recommendations are implemented.

The need for an appropriate balance between the Department's counterterrorism and law enforcement responsibilities and the need to protect civil rights and civil liberties was also highlighted by an OIG report examining the FBI's use of exigent letters and other processes to obtain telephone records without legal process. In addition to prior reports on the FBI's misuse

of national security letters (NSL), in January 2010 the OIG issued a review that examined the extent of the FBI's use of exigent letters and other informal requests, rather than properly issued NSLs, to obtain telephone records between 2003 and 2006. We found misuse of exigent letters and widespread use of other improper and even more informal requests for telephone records, such as requests made by e-mail, face to face, on post-it notes, and by telephone. The FBI also had obtained telephone records using a practice referred to by the FBI and the providers as "sneak peeks." Our report described other troubling incidents regarding such requests, including improper requests for reporters' telephone records; inaccurate statements made by the FBI to the Foreign Intelligence Surveillance Court; improper use of administrative subpoenas; and serious lapses in training, supervision, and oversight regarding the use of NSLs.

In response to our reports on NSLs and the use of exigent letters, the FBI has taken significant steps to correct deficiencies we identified. For example, the FBI has implemented an automated system to generate and track NSLs and ensure accurate reports to Congress and the public on NSL usage. The FBI also issued NSL guidance memoranda, conducted training of FBI field and Headquarters personnel on the proper use of NSLs, and created a new Office of Integrity and Compliance modeled after private sector compliance programs. In addition, the Department's National Security Division has instituted periodic national security reviews of FBI field and Headquarters divisions to assess whether the FBI is using various investigative and intelligence techniques, including NSLs, in accordance with applicable laws, guidelines, and policies. We are currently assessing the effectiveness of the FBI's corrective actions in these areas.

The OIG is also conducting additional reviews addressing the challenge the Department faces in balancing its counterterrorism and law enforcement responsibilities with protecting individual civil rights and civil liberties. For example, Section 702 of the *Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008* (Act) authorizes the targeting of non-U.S. persons reasonably believed to be outside the United States to acquire foreign intelligence information. The Act requires the OIG to examine the number of disseminated FBI intelligence reports that contain a reference to a U.S. person identity, the number of U.S. person identities subsequently disseminated in response to requests for identities not referred to by name or title in the original reporting, the number of targets later determined to be located in the United States, and whether communications of such targets were reviewed. Our review is also examining the FBI's compliance with the targeting and minimization procedures required under FISA.

In sum, the Department must continually focus on implementing appropriate training, policies, controls, and oversight mechanisms to make certain that the Department protects civil rights and civil liberties while at the same time aggressively pursuing its counterterrorism and law enforcement responsibilities.

5. Information Technology Systems Planning, Implementation, and Security: The Department's planning, implementation, and security of its information technology (IT) systems form an increasingly difficult challenge, and the Department's track record in this area is uneven.

The Department annually spends almost $3 billion on planning, implementing, and securing its many complex IT systems. The Department must plan those systems so that they keep pace with technological innovations and meet the changing IT needs of the Department. At the same time,

the Department must seek to implement those systems in a timely and cost-effective fashion and ensure the security of those systems.

As noted in previous years' top management challenges, the Department has experienced significant problems in developing and implementing these IT systems. Several of the Department's major IT initiatives have failed to meet their objectives after hundreds of millions of dollars were expended. Some of these IT systems have taken so long to develop that they were technologically outdated by the time they were ready to be implemented.

Yet, the Department still uses a decentralized system for development of IT projects, which results in higher costs and duplicate IT solutions to common business processes. The Department IT Investment Review Board (DIRB), which is chaired by the Deputy Attorney General, attempts to monitor the progress of the Department's most important IT investments and annually reviews each component's IT investment portfolio. However, the DIRB's lack of direct line authority over IT project development makes it dependent on the components for information about IT projects and reduces its ability to prevent problems in the development of IT systems.

As evidence of the Department's difficulties in this area, in August 2010 the Office of Management and Budget (OMB) issued a list of 26 high-risk IT projects across the federal government that "experienced problems such as significant cost increases or schedule delays." That list contained three Department projects – the FBI's Sentinel Project to develop a case management information system, the Justice Management Division's Litigation Case Management System (LCMS) project to develop a case management information system for all seven of the Department's litigating divisions, and the FBI's Next Generation Identification (NGI) project to develop a state-of-the-art automated system for sharing fingerprint and other biometric information. We share OMB's concern over these three IT systems.

With regard to Sentinel, when the FBI awarded a contract to Lockheed Martin in March 2006 to develop Sentinel, the FBI estimated that it would cost a total of $425 million and be completed by December 2009. In a report issued in October 2010, the seventh of our reports on the development of Sentinel, we found that Sentinel is at least 2 years behind schedule and at least $100 million over budget. According to its original plan, Sentinel was to be fully completed by now. However, after spending about $405 million of the $451 million budgeted for the Sentinel project, the FBI has delivered only two of Sentinel's four phases to its agents and analysts. Moreover, we believe that the most challenging development work for Sentinel still remains.

The FBI recently announced a new plan for completing Sentinel. According to this new plan, the FBI will employ a new "agile methodology" and assume direct management of Sentinel development, reducing the role of Lockheed Martin as the prime contractor. Our initial consideration of the plan raises significant concerns and questions about the FBI's approach, including concerns relating to the cost, schedule, and amount of work to complete Sentinel. We are also concerned that budget and schedule constraints might reduce the functionality ultimately delivered to the FBI's agents and analysts. We will continue to monitor the progress of Sentinel.

The second high risk Department project identified by OMB, the LCMS project, has been under development since 2004. LCMS, which was intended to be a centralized IT case management

system for approximately 14,500 authorized users in the Department's seven litigating divisions, was originally estimated to cost about $42 million and to be completed by December 2010. Yet, in an audit report issued in March 2009 we found that the LCMS project was more than 2 years behind schedule, approximately $20 million over budget, and at significant risk of not meeting the Department's requirements for litigation case management.

The reasons for the delays and cost overruns in LCMS were similar to problems we have identified with the implementation of other Department IT systems. Specifically, we found an ineffective requirements planning processes for LCMS, requirements being modified after much work had been done, defects identified in system integration and user acceptance that were costly to correct, and the failure to adequately address in a timely fashion the difficulties the contractor was having in meeting schedule and cost requirements. Because of these deficiencies OMB's Chief Information Officer recently reported that the Department has decided to terminate the LCMS project. As a result, millions of dollars in development of this IT system were spent in an unsuccessful attempt to develop a consolidated system, and the Department still struggles with decentralized, disparate litigation case management systems.

The third Department high-risk project identified by OMB is the FBI's Next Generation Identification (NGI) project, which is intended to enhance the existing capabilities of the FBI's current fingerprint identification system and provide searching capability for other types of biometric identification, such as palm prints, iris scans, and tattoos. NGI is intended to significantly reduce the amount of time needed to conduct searches for high-priority records. The FBI has requested $2.7 billion for this project from FY 2006 through FY 2010, and the project is expected to be completed by 2017. According to the OMB's "Federal IT Dashboard," the total cost of NGI is expected to be $3.4 billion through its completion in FY 2017. One of the key challenges for this high-dollar project is to contain its cost while implementing a design that can accommodate new types of biometric evidence as they become available.

The issues associated with these three projects mirror problems that the Department has experienced in the development of other IT systems. For example, the OIG identified similar IT system implementation issues in a March 2010 OIG review regarding the backlog of forensic analysis of DNA in the FBI Laboratory. Since September 2003, the FBI has spent over $10 million on developing a laboratory information system. Yet, over 6 years later the system is still under development, and the FBI Laboratory is incapable of generating an electronic chain-of-custody document, tracking laboratory-wide evidence workflows, or producing laboratory-wide statistical reports to identify problems and delays.

Another example of a difficult major IT development project is the Department's Integrated Wireless Network (IWN), a joint project with the Department of Homeland Security (DHS) and the Department of Treasury (Treasury) that is intended to allow federal law enforcement agents to communicate across agencies. This project is seeking to permit interoperability with state and local law enforcement partners, and meet mandates to use federal radio frequency spectrum more efficiently. In March 2007, the OIG reported that the project, which at that time had a budgeted cost of $5 billion between the Department, DHS, and Treasury, was at high risk for failure due to weaknesses in the program's governing structure and the uncertain and inconsistent funding mechanisms that allowed the participating agencies to pursue separate solutions. Now it appears

that the development of IWN is still struggling. We are currently conducting an audit of the IWN project to evaluate the cost, schedule, and implementation of the IWN program.

Another example of an IT system under development that presents major challenges and must be carefully monitored is the Department's Unified Financial Management System, which is intended to standardize and streamline financial processes across the Department. The Department currently uses six major accounting systems that are not integrated with each other. These disparate legacy systems prevent the Department from easily obtaining current, detailed, and accurate financial information about the Department as a whole. The challenges in the development of a Unified Financial Management System are discussed more fully in the financial management challenge discussion.

When developing IT systems, the Department also must make certain that they are secure. The Department must ensure that IT developers and integrators have a clear understating of a system's requirements, that staff implement and continuously monitor security controls, and that adequate funding is available throughout the system's lifecycle to maintain the system's certification and accreditation.

In sum, developing IT systems in a timely, cost-effective, and secure way remains a major challenge for the Department. The difficulties the Department is facing are similar to the problems in other federal agencies, and there are no quick and easy solutions. But the Department's track record in this area is uneven, and we believe the Department must focus on this increasingly important challenge.

6. Violent and Organized Crime: While focusing on counterterrorism, the Department must also continue to address violent and organized crime. Organized crime in particular presents challenges for the Department because it is responsible for a wide range of criminal activity, such as manipulation of financial markets, drug trafficking, prostitution and human trafficking, and violent crimes, and has taken on an increasingly transnational nature. Organized criminals can launch their attacks from around the globe, which presents significant challenges for the Department's law enforcement efforts.

One type of organized crime – gang-related crime – has increased in prevalence and scope. According to the February 2010 National Drug Threat Assessment, in 2009 there were an estimated 1 million members belonging to over 20,000 criminally active gangs within the United States. The 2009 National Gang Threat Assessment reported that criminal gangs commit as much as 80 percent of the crime in many communities.

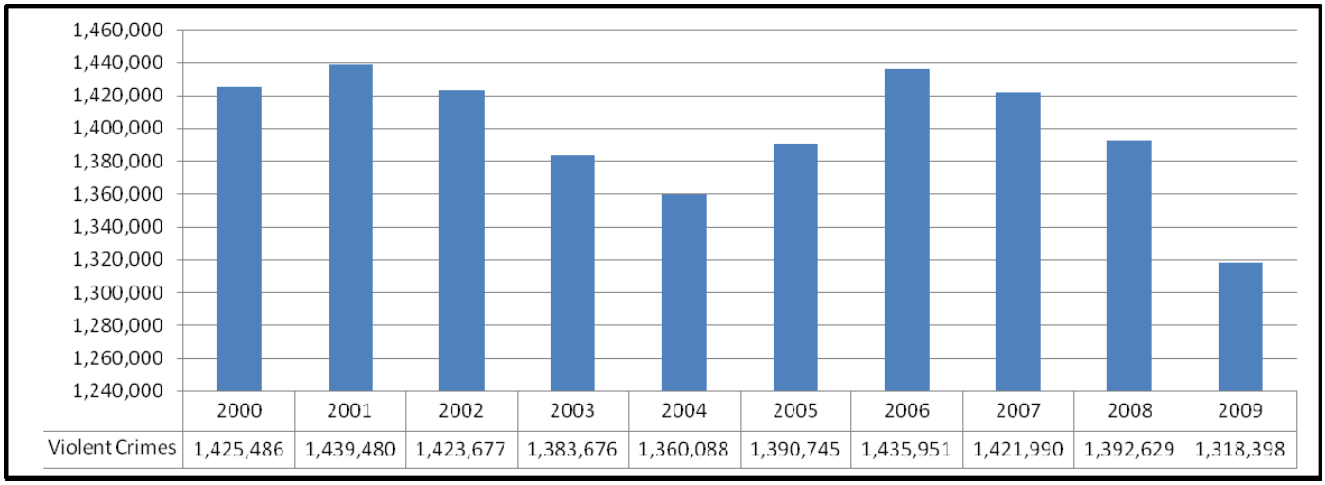
To combat violent gangs, among other measures, the Department established the National Gang Intelligence Center (NGIC) and the National Gang Targeting, Enforcement, and Coordination Center (GangTECC). NGIC, which is administered by the FBI, is a multi-agency center that develops and shares gang-related information among federal, state, local, and tribal law enforcement agencies. GangTECC, which is administered by the Criminal Division, is a coordination center for multi-jurisdictional gang investigations. Partnership of these two centers was intended to provide investigators and prosecutors with "one-stop shopping" for intelligence on gang activity and assistance with gang prosecutions.

However, an OIG review in November 2009 found that NGIC and GangTECC were not effectively collaborating and were not sharing gang-related information despite being located in the same office suite. Specifically, we concluded that the Department's two gang intelligence and coordination centers had not significantly improved the coordination and execution of its anti-gang initiatives. We also found that NGIC has not established a centralized gang information database as directed by statute due to technological limitations and operational problems, and had not shared gang intelligence and information effectively with other law enforcement organizations.

In response to our review, the Department is establishing a partnership of GangTECC and NGIC with the DEA's Special Operations Division and the Organized Crime Drug Enforcement Task Force Fusion Center. The Department also is considering merging three Criminal Division sections, including GangTECC and the Criminal Division's Gang Unit, to form the Organized Crime and Gang Section. As of September 2010, however, the Criminal Division merger was still pending formal approval by the Department.

Despite the challenges in combating organized crime, we believe the Department's efforts in addressing violent crime, in conjunction with its state and local partners, has shown progress. In 2009, an estimated 1.32 million violent crimes were reported, but this represented a decrease of 5.6 percent when compared with the number of violent crimes reported for 2008 (1.39 million).

Number of Reported Violent Crimes, 2000 - 2009



	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
Violent Crimes	1,425,486	1,439,480	1,423,677	1,383,676	1,360,088	1,390,745	1,435,951	1,421,990	1,392,629	1,318,398

Source: The FBI's 2009 *Crime in the United States* report.

However, challenges remain in combating violent crime. For example, the FBI Laboratory analyzes forensic DNA from crime scenes, which can provide critical evidence in identifying and prosecuting violent criminals. Our recent audit found that the FBI Laboratory's backlog of forensic DNA cases is large and growing. As of March 2010, the FBI Laboratory had a backlog of over 3,200 forensic DNA cases in its Nuclear DNA Unit, which primarily examines biological fluid stains, such as blood and semen, and in its Mitochondrial DNA Unit, which analyzes evidence such as naturally shed hairs, hair fragments, bones, and teeth. From FY 2009 through

the second quarter of FY 2010, the backlog of cases in the Nuclear DNA Unit grew by almost 40 percent, and in the Mitochondrial DNA Unit the backlog of cases grew by almost 130 percent. The length of time it takes for contributors to receive results from the FBI Laboratory after submission of evidence varies from an average of approximately 150 days to over 600 days, depending on the type of submission. This backlog can delay legal proceedings that are waiting on the results of DNA analysis, prevent the timely capture of criminals, prolong the incarceration of innocent people who could be exonerated by DNA evidence, and adversely affect families of missing persons waiting for positive identification of remains.

The FBI reported that it is in the process of hiring additional forensic examiners to address the forensic DNA backlog. However, hiring and training the new personnel could take approximately 12 to 18 months and therefore would not have a significant impact on the current backlog for almost 2 years. The FBI is also pursuing other strategies, such as outsourcing agreements and a laboratory information management system, to address the forensic backlog.

Our report made five recommendations to the FBI to help improve Laboratory DNA operations, such as standardizing FBI Laboratory-wide definitions for calculating backlog, ensuring FBI Laboratory users have access to a laboratory information management system, and examining the effect of outsourcing agreements on the overall backlog and the time contributors wait for test results. The FBI concurred with these recommendations and is developing a plan to implement them.

Another critical service that the Department provides to combat one type of violent crime is the maintenance of the National Sex Offender Registry. Yet, in a 2008 report, we found that information in the National Sex Offender Registry was incomplete and inaccurate, and the registry was not a reliable tool for law enforcement and the public. In response to our report, the FBI initiated audits of state sex offender registries, which are the source of information in the National Sex Offender Registry, to ensure the information contained in the National Sex Offender Registry is complete and accurate and in compliance with FBI procedures and statutory guidelines. In addition, since the issuance of our report, the FBI and USMS have improved procedures for transferring data from the National Sex Offender Registry and the National Crime Information Center's Wanted Persons File from the FBI to the USMS so the information can be used to identify fugitives wanted for offenses related to sex offender registration requirements.

ATF also plays an important role in combating violent crime by ensuring that federal laws are followed during the sale of guns. For example, ATF conducts regulatory inspections of Federal Firearms Licensees (FFLs) to determine whether FFLs are taking appropriate measures to avoid selling firearms to prohibited persons. In a 2004 review, we found that ATF's inspection program was not fully effective for ensuring that FFLs comply with federal firearms laws because inspections were infrequent and of inconsistent quality, and follow-up inspections and adverse actions were sporadic even when numerous or serious violations were identified. We recommended ATF improve its inspection program by developing a standard inspection process, revising staffing requirements, improving the comprehensiveness of crime gun tracing by law enforcement agencies, and creating a tracking system to monitor the progress and timeliness of FFL denials and revocations. We are now conducting a follow-up review to assess the changes ATF has made to the gun dealer inspection program since 2004.

In sum, although violent crime in general has decreased over the past several years, the Department must not relent in its focus on this challenge, and the Department must focus particular attention on the challenges posed by organized criminal groups.

7. Financial Crimes and Cyber Crimes: The need to aggressively combat financial crimes and cyber crimes is an increasing challenge for the Department. Financial fraud continues to affect the economy, and the increased use of computers and the Internet in furtherance of financial crimes, as well as the international scope of these criminal activities, has exacerbated the challenge of cyber crime.

In November 2009, a presidential Executive Order created the Financial Fraud Enforcement Task Force (Task Force). The Department described the Task Force as the "cornerstone" of its work in the financial fraud area. Led by the Department, the Task Force combines the work of several agencies to focus on mortgage crime, securities fraud, *American Recovery and Reinvestment Act* (Recovery Act) and rescue fraud, and financial discrimination.

In connection with the Task Force the Department launched Operation Stolen Dreams, a multi-agency initiative designed to combat mortgage fraud. In June 2010 the Department reported that this operation involved the prosecution of 1,215 criminal defendants nationwide who allegedly were responsible for more than $2.3 billion in losses. The Department also reported that the operation recovered more than $147 million through 191 civil enforcement actions.

The Department and the Task Force are also focusing investigative resources on securities fraud as well as on Recovery Act fraud and fraud in other rescue funds. Among other things, the Department is providing training to federal grantees and contractors on ways to prevent and detect such fraud.

Closely related to the challenge of financial crimes is cyber crime. Rapid technological advances and the widespread use of the Internet make cyber crime an increasing challenge for the Department. The broad range of cyber crime includes online fraud, identity theft, and child pornography. In addition, cyber attacks can threaten national security and also result in serious financial consequences for individuals, businesses, and government institutions. Cyber crime is of particular concern because it can be committed remotely and anonymously, across state and international borders.

Identity theft is a major cause of financial and cyber crime. According to the Department, identify theft was the fastest growing crime in 2008, victimizing more than 10 million Americans. Yet, a March 2010 OIG audit report found that that the Department had not developed a comprehensive strategy to combat identity theft. We also determined that the Department had not implemented several of the recommendations stemming from a 2008 follow-up report issued by the President's Identity Theft Task Force. We recommended that the Department ensure that its efforts to combat identity theft are better coordinated and are given sufficient priority. Since we issued our audit, the Department has designated a senior official to coordinate the Department's identity theft enforcement efforts, and all relevant DOJ components have designated an official to oversee their components' identity theft enforcement efforts.

These officials have held initial meetings and are working to improve the Department's efforts to combat identity theft.

The Department must also focus attention on cyber crime that can threaten national security. The OIG is examining the development and operation of the FBI's National Cyber Investigative Joint Task Force, as well as the capabilities of FBI field offices to investigate national security cyber cases. In addition, we are conducting a separate review on the Departments Justice Security Operations Center, which helps protect the Department's information technology infrastructure and sensitive data from cyber attacks.

Overall, we believe the Department is making progress in combating financial and cyber crime through targeted initiatives and by collaborating with other agencies to combat the mounting challenge. However, this area is a top management challenge for the Department.

8. Detention and Incarceration: Safely, securely, and economically handling the large federal inmate and detainee populations is a difficult challenge for the Department. The Federal Bureau of Prisons (BOP) must contend with overcrowded and aging facilities, higher inmate to staff ratios, the need to address staff sexual abuse of inmates and other types of staff misconduct, and providing jobs and training programs for inmates while they are incarcerated. At the same time, the USMS must find cost-effective detention space in state and local facilities to house tens of thousands of federal detainees awaiting trial or sentencing.

These challenges are even more difficult because of the significant increase in the federal inmate population. In the past 10 years, the inmate population has risen from 156,572 inmates at the end of FY 2001 to 210,227inmates at the end of FY 2010, an increase of 34 percent. The inmate to staff ratio for 2001 was 4.1 to 1 and for 2010 was at 4.82 to 1. Approximately 82 percent of inmates are confined in BOP-operated facilities, with the balance housed in privately managed or community-based facilities and local jails.

This influx of prisoners has led to overcrowding across the BOP prison system with BOP facilities at 37 percent above rated capacity, on average. The greatest growth is in the numbers of medium- and high-security inmates who the BOP cannot house in contract facilities. The BOP must either add beds to existing BOP institutions or build new institutions. Since FY 2006, the Department has identified prison overcrowding as a material weakness in the Department's Performance and Accountability Report. According to the BOP, increases in prison crowding and the inmate to staff ratio are both correlated with increases in violence among the inmate population.

In addition to being overcrowded, approximately one-third of the BOP's 116 institutions are 50 years old or older. Aging facilities often present greater security risks than newer facilities. Many of the BOP's older facilities have never undergone major renovations and require extensive work to maintain compliance with established prison security standards.

Another factor that can affect the safety of inmates and staff is misconduct by correctional officers. One especially serious type of misconduct that undermines the safety and security of prisons – for both inmates and other staff – is staff sexual abuse of inmates. This is not a

harmless or victimless crime. It harms inmates, and it also undermines the security of institutions by corrupting staff members. Of the small percentage of correctional officers who have sexual relationships with inmates, many also smuggle contraband, ranging from cell phones to drugs and weapons, into prisons for these inmates.

In September 2009, the OIG issued a report on the Department's efforts to prevent staff sexual abuse of inmates. Since then, we have continued to assess the BOP's progress in preventing sexual abuse of inmates and providing services to inmate victims. We have found that, in response to our recommendations, the BOP has improved its procedures for tracking allegations, clarified and reinforced prison procedures for providing medical and psychological services to inmate victims, and updated training for inmates and staff. However, of continuing concern are the BOP's procedures for safeguarding inmate victims of sexual abuse. As protective measures, the BOP typically isolates inmate victims in special housing units and transfers victims to other institutions. Yet, these measures may further traumatize victims and move them further away from family members. Alternatives to isolation and transfer are available, and the BOP has agreed to considered alternatives in each incident. However, the BOP has not developed a method to determine whether institutions have appropriately considered alternatives before isolation and transfer are used as protective measures.

Under the *Prison Rape Elimination Act of 2003*, the Department is responsible for reviewing the proposed standards issued by the National Prison Rape Elimination Commission and issuing national standards to enhance the detection, prevention, reduction, and punishment of prison rape. The Act mandated that the Attorney General publish a final rule adopting national standards by June 2010, 1 year from the date of the Commission's recommendations. The Department has not yet met this statutory requirement. The Department is in the process of considering comments to the recommended standards but has not published its final rule. We believe it is essential that the Department move quickly to comply with the Act and implement a final rule to help protect inmates from prison rape.

The BOP's ability to screen out unsuitable applicants when hiring correctional officers is an important safety issue for both inmates and staff members. Last year, 28 BOP officers were convicted of committing criminal acts while on the job, such as sexual abuse of inmates or smuggling contraband into a prison facility. In addition, approximately 80 correctional officers were fired or resigned because of misconduct findings. While these employees represent only a small percentage of the BOP's work force of over 38,000 employees (about half of which are correctional officers), misconduct by even a few employees can undermine the safety and security of institutions and violate the rights of inmates. The OIG is currently examining the BOP's strategies and procedures for hiring correctional officers.

Federal Prison Industries, called "UNICOR," is a government corporation within the BOP that provides employment to staff and inmates at federal prisons throughout the United States. Participation in the UNICOR Program can help reduce inmate misconduct by keeping prisoners productively occupied, and it also can reduce recidivism by providing inmates with marketable work skills. As of June 2010, UNICOR operated 103 factories at 73 prison locations, employing approximately 17,000 inmates. However, the number of inmates who participate in

UNICOR was significantly lower this year than previous years because UNICOR closed and downsized several factories during the past year.

In addition to the challenge of managing UNICOR so that it is financially self-sustaining, the BOP also must ensure that UNICOR facilities provide a safe work environment for inmates and staff. The OIG released a report in October 2010 that found workers and inmates at several BOP institutions were exposed to toxic metals, such as cadmium and lead, and other hazards while working in electronic waste (e-waste) recycling plants operated by UNICOR. Our report, which was completed with the assistance of four federal agencies with expertise in health, safety, and environmental matters, found that UNICOR had significant problems with its e-waste program and exhibited a troubling lack of attention to the safety of staff and inmates who participated in the e-waste recycling operations, especially from the program's inception in the mid-1990s to 2003. However, we also found that UNICOR began to implement significant health and safety improvements to its e-waste recycling operations starting in June 2003, primarily to control exposures to toxic metals. Our review determined that by 2009, with limited exceptions, UNICOR's e-waste operations were compliant with Occupational Safety and Health Administration requirements and were being operated safely. The OIG and the agencies that assisted us made various recommendations that can help UNICOR further improve its compliance with applicable health, safety, and environmental requirements. The BOP concurred with those recommendations and is beginning to implement them.

The OIG also recently reviewed the BOP's furlough program, which is used to transfer inmates to another BOP institution, a medical facility for long-term treatment, or a halfway house when the inmates are nearing the end of their sentences. The BOP also uses non-transfer furloughs, where inmates are allowed to leave and return to the same institution, to permit inmates to receive short-term medical treatment, strengthen their family ties, or allow them to participate in educational, religious, or work-related activities.

Our report, issued in September 2010, found weaknesses in the BOP's policies regarding the furlough program. Most significantly, the BOP's current furlough policy does not require BOP staff to notify victims and witnesses when an inmate is released on a medical furlough, does not require inmates to sign a document specifying that a urinalysis test will be conducted upon the inmate's return from the furlough, and does not contain limitations on the furlough eligibility of inmates found guilty of drug use or the introduction of drugs into BOP institutions.

We also determined that the BOP drafted a policy in 2003 to address these and other weaknesses in its furlough program. However, the BOP has not implemented this draft policy for over 7 years because, according to BOP officials, the BOP must negotiate policy changes with the union representing BOP employees before implementing the changes, and this draft policy never reached the top of the queue for negotiation. Therefore, 7 years after the BOP drafted a policy that addresses weaknesses in the furlough program, the policy has yet to be implemented. Moreover, in response to our report, the BOP estimated that the revised furlough policy would not be negotiated and implemented until December 2017. We believe that the BOP's timeframe for implementation of this recommendation is excessive and unacceptable. In essence, the BOP's response to our recommendation is stating that it will take a total of 14 years before

important improvements to its furlough policy, including one that would enhance victims' rights, are implemented.

When our report was issued, the union representing BOP employees stated that BOP management was at fault because it failed to use a mechanism to prioritize this issue for negotiations. According to the BOP, there are approximately 50 other items on the list to be negotiated, including important issues such as searches of BOP staff for contraband, procedures related to the BOP witness security program, and staff discipline procedures.

We believe that it is critical for the BOP and the union to address expeditiously outstanding issues, including the furlough program and other issues that can affect the safety and security of prison staff and inmates. We also believe that the negotiating process needs to be revised to allow the issues to be addressed in a timelier manner.

In addition to incarcerating sentenced inmates at BOP facilities, the Department also must provide safe and affordable detention space for nearly 60,000 federal detainees awaiting trial or sentencing. The USMS is responsible for housing these detainees, and the Department's Office of the Federal Detention Trustee (OFDT) oversees approximately $1 billion in the annual budget for housing federal detainees. The USMS houses 80 percent of its detainees in non-federal detention space. To do so, it negotiates contracts, known as Intergovernmental Agreements (IGA), with approximately 1,800 state and local governments.

Over the years, we have expressed concerns that the Department was not effectively negotiating the rates it pays to state and local entities for housing these federal detainees. In FY 2008, the OFDT and USMS made changes in the way they establish jail-day rates with state and local detention facilities. One change involves OFDT using an econometric statistical model, known as eIGA, for estimating a fixed-price range for the jail-day rate for federal detainees housed at state and local facilities. However, negotiated jail-day rates under the new approach appear to give some state and local facilities a large profit to house the detainees. We are conducting an audit reviewing the Department's use of the eIGA process to determine whether it is economically and efficiently setting the jail-day rates. This issue can have significant consequences for the total budget required to house detainees.

In sum, the Department continues to face difficult challenges in providing adequate prison and detention space for the increasing prisoner and detainee populations and in maintaining the safety and security of prisons.

9. Grant Management: The OIG has included grant management as a top management challenge since the inception of this list. Beginning in 2009, the Department faced heightened challenges in grant management because it had to award $4 billion in grants under the Recovery Act at the same time that it had to award the $3 billion in grant funding contained in the Department's annual appropriations.

For 2010, we report a single challenge that focuses on the Department's management of grant funds in the Recovery Act as well as the Department's regular grant programs.

The Recovery Act, which provided $787 billion in total funding to attempt to stimulate the economy, included $4 billion in Department grant funding to enhance state, local, and tribal law enforcement; to combat violence against women; and to fight Internet crimes against children. As of the end of August 2010, the Department had expended about 52 percent of its Recovery Act funds. The Department handled this increased grant workload without any significant increase in staff. Our reviews have found that, in general, the Department's grant management staff made extraordinary efforts to implement the Recovery Act programs and generally issued the Recovery grant funds in a timely, fair, and objective manner.

At the same time, the Department has sought to improve its regular grant management practices. In 2009, shortly after the passage of the Recovery Act, the OIG developed a document, entitled *Improving the Grants Management Process,* which contains a series of recommendations and best practices in grant management that federal agencies should consider implementing. The Department responded positively to the recommendations in this document and has implemented changes in its grant management practices, including expanding the use of online training opportunities among grant recipients and assisting grantees in determining the appropriate performance information to collect. In addition, the Department's Office of Justice Programs' (OJP) Office of Audit, Assessment, and Management has improved the Department's monitoring and oversight of grants by: (1) establishing a working group to review monitoring practices and develop standard monitoring approaches and procedures, (2) enhancing computer systems and developing new procedures for managing grant programs, (3) updating oversight and monitoring procedures, and (4) improving site visit documentation and the quality of site visit reports.

This past year, when the Department planned to expand the number of grants awarded to tribal organizations, the Department asked the OIG for additional recommendations relating specifically to tribal grant management and oversight. In response, the OIG drafted a document, entitled *Improving the Grant Management Process for Department of Justice Tribal Grant Programs,* which provided additional recommendations for the Department to consider, such as increasing training, assistance, and oversight to tribes with inadequate accounting systems.

While we believe the Department has taken positive steps toward improving its grant management practices, these changes will take time to fully implement and to incorporate into the Department's regular practices. Moreover, our audit work has continued to identify areas where the Department could further improve its management of grants. For example, our audits of Recovery Act programs found that the Department's program offices and bureaus did not always assess the programmatic, financial, and administrative areas of the grants before making awards, and they also did not retain adequate documentation to support their review work.

In addition, the Department needs to ensure that grant applicants submit key documents in their application packages. For example, our review of OJP's administration of the Byrne Grant Program, which provided $2.2 billion in both formula and discretionary Recovery Act grants to states, tribes, and local governments to support a broad range of law enforcement activities, found that OJP generally managed the Recovery Act funds for the Byrne Program in accordance with OMB guidelines and established grant management practices. However, we also found that

OJP awarded several formula grants to applicants whose packages were missing key documentation, such as complete program narratives, project abstracts, and budget documents. OJP also treated competitive grant applicants inconsistently, allowing some grant applications to continue through the competitive process even though they did not meet one or more of the solicitation requirements, while denying other applicants further consideration for the same deficiencies. OJP agreed to implement procedures to ensure that applications are treated consistently when OJP reviews applications to determine whether they meet the application requirements.

The Department should also implement better controls to ensure that it correctly scores grant applications. For example, in May 2010 we issued an audit report on the selection process for the $1 billion Community Oriented Policing Services (COPS) Hiring Recovery Program, which awards grants to state and local entities for the hiring, rehiring, and retention of career law enforcement officers. Our audit determined that COPS used inaccurate formulas in developing the scores and ranks of applicants, which resulted in the allocation of grants to 45 entities that should not have received grants, while another 34 entities that should have received grants did not. In addition, we identified six grantees that received more officer positions than they should have and six grantees that received fewer officer positions than they should have. In response to our audit, COPS informed us that it has corrected the formulas for future use and modified its FY 2010 hiring grant allocation process to ensure that those entities that were negatively affected due to scoring inaccuracies received appropriate grant funding. We plan to review these actions taken by COPS.

We found a similar calculation error in our audit of the Office on Violence Against Women's (OVW) administration of $225 million in grant funding. Our audit determined that the OVW had awarded its grants in a prompt and reasonable manner, but we identified several instances where OVW internal peer reviewers incorrectly tabulated individual application scores and thus incorrectly ranked some applications higher than others. In addition, we found that peer reviewers were not always screened for potential conflicts of interest before they were allowed to evaluate and score discretionary grant applications.

We also found in our Recovery Act audits that the Department was not consistently documenting its reasons for making discretionary awards and was not explaining why some applications that were ranked lower by peer reviewers were awarded grants over applications that peer reviewers had ranked higher. Although the Department is not required to follow the rankings of peer reviewers in awarding grants, we believe that the Department should document its rationale for award decisions that deviate from peer review results.

Our other recent oversight work on non-Recovery Act funds identified areas where the Department can improve its grant management. In July 2010, we issued a report on OJP's management of its offender reentry initiatives, programs which seek to reduce inmate recidivism and to help state, local, and community organizations provide assistance to released inmates as they transition to life outside prison. Our audit found that OJP had not established an effective system for monitoring grantees to assess whether they were meeting program goals. In response to the audit, OJP has taken steps to make grantees aware of reporting procedures to facilitate timely and accurate reports, provided detailed and precise definitions to current reentry grant

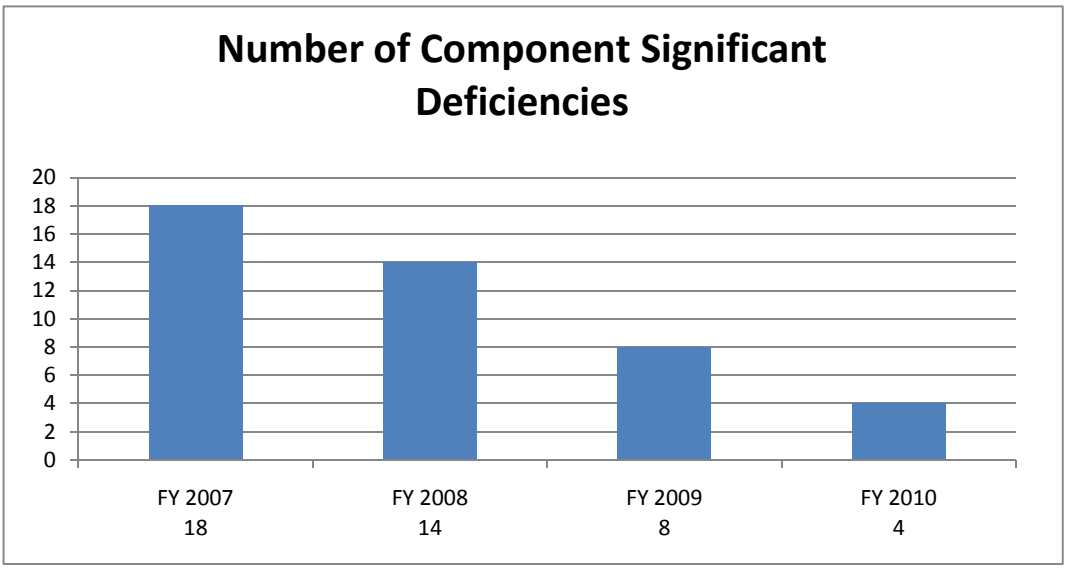
applicants regarding target populations, and to evaluate the current reentry grant program. In our individual audits of grantees' use of awarded funds, we determined that the use of some grant funds were not supported by documentation, were unallowable based on the terms and conditions of the grant, or were not used for appropriate grant expenditures.

We also believe that the Department can take further action to address outstanding recommendations to resolve questioned costs from our audits of grantees. For example, we released an audit report in 2006 on the Department's grant closeout process in which we recommended that OVW resolve $37 million in questioned costs related to grant drawdowns occurring more than 90 days past the grant end date and de-obligate and put to better use over $14 million obligated to expired grants that were already 90 days past the grant end date in 2006. We have had multiple communications with OVW about this issue since we issued our report in 2006, but OVW has yet to resolve these recommendations.

In sum, we believe the Department is demonstrating a commitment to improving its grant management process, and we have seen significant signs of improvement in this area. However, further improvements are needed, and considerable work remains before managing the billions of dollars the Department awards annually in grants is no longer a top challenge for the Department.

10. Financial Management: Financial management has been a top management challenge for the Department since 2003. It is important to recognize that the Department has made significant improvements in its internal controls over financial reporting and management at the same time there has been an increasing demand for accountability and transparency in these financial systems. Yet, we believe the need for accurate, near real-time financial information continues to present management challenges for the Department.

For FY 2010, the Department again earned an unqualified opinion and improved its financial reporting. For the fourth straight year the financial statement auditors did not identify any material weaknesses at the consolidated level. Department components also reduced component significant deficiencies from eight in FY 2009 to four in FY 2010.



As in 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 and cost of these ad hoc and labor-intensive efforts, which are often overlooked in measuring the true costs of maintaining the current financial management systems.

The decentralized structure of the Department also presents a major challenge to obtaining current, detailed, and accurate financial information about the Department as a whole because there is no one single source for the financial data. The Department currently uses six major accounting systems that are not integrated with each other. In some cases, the components' 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 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 and satisfy other financial data submission requirements until automated, integrated processes and systems are implemented that readily produce financial information throughout the year.

The Department has long recognized the need for a Department-wide financial management system and has sought to implement a Unified Financial Management System (UFMS) to replace the disparate major accounting systems currently used throughout the Department. 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.

Yet, only the DEA has fully implemented the UFMS, with ATF scheduled for full implementation during FY 2011. Successfully implementing the UFMS at the DEA is a significant achievement, although the DEA's legacy system was one of the most modern

financial management systems within the Department. Likewise, ATF has one of the Department's most modern systems. Thus, the central issue to this challenge remains largely unaddressed because the Department's other components continue to use non-integrated and, in some cases, antiquated financial management systems.

Implementation of the UFMS at the USMS, which has one of the most antiquated legacy financial management systems, began in FY 2010 and will continue through FY 2012. Moreover, based on recent OMB guidance, the implementation of the UFMS at the FBI, which has another antiquated legacy financial management system, is uncertain. At the request of OMB, the Department has begun detailed discussions with the Financial Systems Advisory Board (FSAB), which advises OMB about IT development. FSAB is conducting a review of pending agency financial system IT projects. We understand that FSAB supports DOJ's desire to further consolidate its financial management systems, but it also recognizes that the size and cost of the project presents significant risk of failure and excessive cost in implementing the UFMS. In particular FSAB recommended further disaggregation of the various milestones associated with implementing the UFMS at the Department, and that the Department perform further analysis of the operation and maintenance portion of the enterprise-wide implementation of the UFMS.

In sum, while the Department continues to show improvement in its overall financial management, some Department components still lack updated financial management systems. The Department needs accurate, near real-time financial information, and we believe it will be difficult to meet this demand until the Department replaces its antiquated, paper-based systems with modern systems that are technically sufficient.

This page intentionally left blank.