Top Management and Performance Challenges in the Department of Justice - 2011

November 8, 2011

MEMORANDUM FOR: THE ATTORNEY GENERAL
THE DEPUTY ATTORNEY GENERAL

Cynthia A. Schnedar

FROM: CYNTHIA A. SCHNEDAR
ACTING 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) 2011 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.

While the challenges are not presented in priority order, similar to past years we continue to believe that *Counterterrorism* presents the greatest challenge to the Department. In addition, we added the challenge of *Implementing Cost Savings and Efficiencies* in recognition of the difficult challenges the Department faces in continuing to execute its mission in this constrained fiscal climate. In recognition of the fact that 2011 was the fifth straight year that the Department earned an unqualified opinion on its consolidated financial statements with no material weakness, we have removed the challenge of *Financial Management* from the top 10 list. In addition, we have re-categorized two of last year's challenges so that the issues previously represented by *Organized Crimes* and *Financial Crimes and Cyber Crimes* are represented in this year's list as *Criminal Law Enforcement* and *Financial Enforcement*.

We wish to emphasize that all 10 challenges are critical, and many are closely related to each other. For example, we believe that the challenges of combating terrorism, enforcing criminal law, and managing detention and incarceration cannot be addressed in isolation, but rather must take into account the challenge of protecting civil rights and civil liberties. Similarly, many of this year's top 10 challenges relate to fiscal responsibility and resource management, such as *Implementing Cost Savings and Efficiencies*; *Information Technology Systems Planning, Implementation, and Security*; *Financial Enforcement*; and *Grants and Contract Management*.

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

Attachment

---

1. **Counterterrorism:** Ten years after the anniversary of the terrorist attacks on September 11, 2001, counterterrorism remains the highest priority of the Department of Justice (the Department). The deaths of al-Qaeda leaders, including the May 2011 death of Osama Bin Laden, have not affected the goal of al-Qaeda and other terrorist groups to conduct attacks inside the United States. In June 2011, the Administration's Strategy for Counterterrorism noted that the significant terrorist threat posed by al-Qaeda, its affiliates, and its adherents requires the United States and its partners to develop and pursue more agile and adaptive methods to defeat it. In addition, domestic terrorism also remains a significant concern, as illustrated by the January 2011 discovery of an improvised explosive device alongside a parade route in Spokane, Washington, and by the increasing dangers posed by anti-government militia extremism. Although the country and the Department have made considerable progress over the past decade to combat terrorism, the present era of budget and deficit reduction means that significant challenges remain in protecting the country from those who would do it harm while not shortchanging the Department's other important missions.

   Examination of the circumstances of the September 11 attacks makes it clear that the Department must ensure that it accurately processes, manages, and shares the information it has regarding known and suspected terrorists. The Office of the Inspector General (OIG) is conducting multiple reviews and audits to assess how the Department manages information relating to counterterrorism. For example, we are examining the Federal Bureau of Investigation's (FBI) management of the terrorist watchlist nominations process and its encounters with individuals on the watchlist. In a previous audit, the OIG concluded that the FBI did not nominate known or suspected terrorists to the watchlist in a timely manner and did not update or remove watchlist records as required. The current review follows up on our prior audit to ensure that the FBI is making adequate progress to improve this important program. It is critical that the watchlist contain accurate and up-to-date information because it is used by government personnel to determine how to respond when a known or suspected terrorist requests entry into the United States. The OIG is also examining the FBI's Foreign Terrorist Tracking Task Force (FTTTF) to determine if the FBI has implemented a viable strategy to locate and track suspected terrorists and their supporters; if the FTTTF's coordination with law enforcement, intelligence agencies, and other outside entities has enhanced its abilities; and if the FBI has appropriately managed terrorist-related information maintained by the FTTTF.

   Accurate tracking of counterterrorism efforts is also essential to the management of Department resources, as Congress and the Department use statistical reports relating to terrorism to make operational and funding decisions to support the Department's annual budget requests for counterterrorism activities. Particularly in

this time of constrained budgets and deficit reduction efforts, it is essential that the Department report with precision terrorism-related statistics, such as the number of individuals charged with terrorism as a result of terrorism investigations and the number of threats made against people, cities, and transportation facilities. The OIG is conducting a follow-up audit of the Department's internal controls over terrorism reporting to determine whether the National Security Division (NSD), the Executive Office for United States Attorneys, and the FBI have taken appropriate actions to implement the recommendations from our 2007 audit that found that Department components and the Department as a whole did not accurately collect and report terrorism-related statistics. Four of the recommendations we made in that prior audit remain open, including that the FBI ensure terrorism-related statistics are not reported unless evidence is maintained to support the statistics. Our follow-up audit seeks to determine what progress has been made toward closing our recommendations and to determine whether the other corrective actions the Department has implemented have improved the components' ability to gather, track, classify, verify, and report accurate terrorism-related statistics.

Terrorists and criminal hackers are increasingly using the freedom and anonymity of the Internet to threaten national security, and their evolving methods require ongoing adaptation by the Department and the FBI. In April 2011, the OIG published a report examining the FBI's ability to address the threat of cyber intrusions intended to compromise national security. The report focused on the FBI's efforts to develop the National Cyber Investigative Joint Task Force (NCIJTF) and the capabilities of FBI field offices to investigate national security cyber intrusion cases. While our audit found that the FBI had completed the interim goals for the NCIJTF, such as identifying techniques and tactics being used to attack computer networks and incorporating intelligence and law enforcement community partners into the day-to-day operations of the task force, we also identified areas where the NCIJTF could improve its capabilities to defend against cyber attacks. For example, information sharing, even among task force members, was a significant concern. We found that the NCIJTF did not always share relevant information about cyber threats among the task force's partner agencies even though the agencies are co-located at the NCIJTF and are expected to work together daily to mitigate and neutralize cyber threats. Some agencies' representatives were often asked to leave NCIJTF threat focus cell meetings to limit dissemination of information. Further, our audit found that NCIJTF partner agencies had not agreed to a consistent information sharing framework, leaving NCIJTF partner agencies with potentially divergent understandings about what information would be shared.

In addition, we found that FBI field agents often lacked the technical skills necessary to investigate cyber intrusion cases, and many agents believed they did not have time to take the required training to gain these skills. Effective information sharing and proper training are critical to an effective counterterrorism strategy in general, and particularly with regard to cyber intrusions. Our report made 10 recommendations, including that the FBI consider creating a new "cyber intrusion" career path and establish regional hubs staffed with cyber intrusion experts to ensure that the Department has appropriate specialists to address this emerging threat. The FBI has indicated that it agrees with all 10 recommendations, and the OIG will continue to monitor this important issue.

Investigation and prosecution of terrorist financing also play an important role in the Department's efforts to disrupt terrorist organizations and prevent terrorist

attacks. The FBI and NSD share responsibility for identifying, investigating, and prosecuting persons and entities providing financial support to terrorist organizations and in providing operational support and legal guidance to federal, state, local, and international entities. The OIG has initiated a review of FBI and NSD efforts to combat terrorist financing that will examine whether the FBI and NSD are appropriately handling and coordinating these important responsibilities.

In addition, the Department must ensure that it is prepared to respond in the event of a terrorist attack. Since the publication of our June 2010 report concluding that the Department as a whole needed to improve its preparedness to respond to a weapon of mass destruction incident, the Department has formed an Emergency Preparedness Committee to assess its emergency preparedness policies and procedures, and to implement the recommendations made in our report. Those recommendations included designating a leader in the Department with the authority to manage the entire response program and updating the Department's response policies to conform them to the National Response Framework and National Incident Management System. However, 18 months after the creation of this committee, all five of the recommendations we made to the Department remain open. We believe that the Department will be better prepared to ensure public safety in the event of a terrorist attack when this work is complete.

Finally, coordination between the FBI and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) in the event of a terrorist attack involving explosives remains a significant concern. We first raised these issues in our October 2009 review of the coordination between the FBI and ATF in responding to explosives incidents. While the FBI and ATF have made efforts to address the problems identified in our report and the Department has assigned lead jurisdiction over terrorism-related explosives investigations to the FBI, important questions remain. The questions include what ATF's investigative role will be when an explosion's nexus to terrorism is in dispute and which component will have lead agency jurisdiction over non-terrorism crimes that have historically been investigated by the FBI, such as bank robberies. The Department must resolve these coordination issues promptly.

In sum, the effective management of counterterrorism efforts remains a fundamental challenge for the Department. Although the Department's commitment to combating terrorism has been robust and steady, its management of such critical matters as information sharing and agency coordination can be substantially improved.

2. **Implementing Cost Savings and Efficiencies:** The Congressional Budget Office estimates that the United States is facing an enormous budget deficit of $1.28 trillion in 2011, and there are significant pressures to reduce this deficit. During the past fiscal year, two potential government shut downs were narrowly averted by last minute bipartisan agreements, which included the establishment of a "Super Committee" of Members of Congress appointed to find ways to deeply cut the federal budget. Within the current fiscal environment of reduced budgets, hiring and pay freezes, and deficit reduction, it is essential that the Department manage its resources as efficiently and effectively as possible by streamlining or eliminating duplicative or ineffective programs and ensuring that expenditures directly support its mission.

To its credit, the Department has already taken steps to eliminate duplicative programs and reduce costs. In July 2010, the Attorney General created the Advisory

Council for Savings and Efficiencies (the SAVE Council), which helps the Department identify and implement best practices for saving taxpayer dollars, realizing efficiencies, and monitoring Department progress. The Department has estimated that the SAVE Council has saved more than $51 million. Most recently, the Department announced more than $130 million in cost savings and efficiency measures (which include the previously mentioned $51 million) that it intends to implement, such as consolidating Antitrust Field Division offices and merging the Justice Management Division's strategic planning and management functions. Additionally, in January 2011, Attorney General Holder issued a memorandum ordering a Department-wide temporary hiring freeze and instructing components to limit travel, training, and conference spending to only those needs that are essential. The Department also has announced that it will realign functions in various offices, lower lease costs by consolidating or reducing office space, and continue to look for ways to more effectively use the Department's resources. The Department's efforts to identify cost savings are commendable.

Yet more can be done. We believe that the Department also could achieve significant cost savings if it were to consolidate and streamline its efforts in programs with comparable characteristics. For example, as we described in our 2009 report regarding explosives investigation coordination between the FBI and ATF, the Department should consider consolidating its explosives training facilities, including the facilities used to train explosives-detecting canines, as well as Department laboratories that perform explosives-related analyses. In addition, the Department maintains three components that award grants – the Office of Justice Programs (OJP), the Office on Violence Against Women (OVW), and Community Oriented Policing Services (COPS). In our March 2011 report regarding the Department's efforts to monitor and oversee grants awarded through OJP, we found that OVW and COPS perform certain monitoring and oversight functions that are duplicative of the services available through OJP.

In addition to streamlining duplicative programs and consolidating office space, the Department must also negotiate its contracts in a manner that maximizes the value it receives. For example, the Department spends over $1.2 billion a year on non-federal detention space, an amount that has continued to increase each year even though the number of detainees has remained relatively constant. We have repeatedly expressed concern that the Department was not effectively negotiating the rates it pays to house federal detainees. In our March 2011 report regarding the Department's process for negotiating the rates it pays to state and local governments to house detainees, we described significant deficiencies in the United States Marshals Service's (USMS) negotiation strategy tools. For example, although the USMS collects operating expense data from jails showing how much each spends to house detainees, it did not consistently use this data to negotiate lower rates. In addition, we found that during negotiations, the USMS inconsistently applied pricing factors such as independent estimates and rates charged by nearby jails and, in some cases, proposed rates were compared only to the highest rates in a particular area without regard to whether facilities were comparable in terms of type, size, and location. We also identified instances in which some state and local governments took advantage of circumstances such as a shortage in detention space to demand unjustifiable increased rates. We therefore made several recommendations to help the Department better negotiate, justify, and document agreements to obtain non-federal detention space that could result in significant cost savings, including moving detainees to different facilities when a local facility demands an unjustifiable rate

increase. It is essential that the Department collect and use accurate and up-to-date information in this program and others to ensure it is in the best position when it negotiates with contractors and vendors what it will spend on its programs.

During fiscal year (FY) 2011, the OIG issued several reports that highlighted other, smaller expenditures that the Department should analyze to identify opportunities for cost savings. For example, the OIG conducted an audit of how much the Department spends on conference planning and food and beverage costs. The Department reported that it hosted or participated in 1,832 conferences in FYs 2008 and 2009 at a total cost of $121 million. Our audit found that the Department spent approximately $600,000 in grant funds to procure event planning services for five conferences without demonstrating that these firms also offered the most cost-effective logistical services and that two of the Department's components did not collect salary and benefit cost data from their event planners. We also identified unallowable and unnecessary event planning costs. We recommended that components ensure that the Department uses training and technical assistance providers, who are generally more skilled than needed for providing purely logistical services, to plan conferences only when it is the most cost-effective method of providing logistical services, and that recipients of Department funds for conference planning be required to track their time and activities associated with such services. The Department should ensure it is receiving good value for the considerable sums of money it spends on conferences. In response to our report, the Department is taking action to control future conference expenditures. For example, the Justice Management Division (JMD) is issuing guidance to Department components requiring them to conduct a cost-benefit analysis when justifying ordering food and beverages to obtain free meeting space. In addition, Department components are implementing guidelines regarding conference food and beverage limits for conferences supported with cooperative agreement funds that are congruent with Department-wide rules.

The Department can also control expenditures through oversight to ensure that expenses are incurred in accordance with Department policy and government regulations. In November 2010, the OIG issued a report that found while the large majority of U.S. Attorneys rarely or never exceeded the government lodging rate, a small number of U.S. Attorneys routinely exceeded the government rate by large amounts, with insufficient justification. We also found that deficiencies and inconsistencies in the Department's travel policies enabled U.S. Attorneys to authorize their own travel, including authorizing themselves to exceed the government rate. As a result of this review, the Department issued a new policy clarifying the requirement that U.S. Attorneys obtain authorization for their travel from the Executive Office for United States Attorneys. The Department reports that it is implementing new procedures to ensure that U.S. Attorneys, and all Department employees, receive authorization for travel only when necessary and that all related travel expenses are incurred in accordance with government and Department travel regulations. We will continue to monitor their efforts in this area.

Fiscal responsibility is always important, and never more so than in difficult economic times when the Department must fulfill its mission despite budget constraints. The Department must remain innovative and vigilant in continuing to identify opportunities to increase efficiencies, eliminate ineffective programs, and direct funding toward its highest priorities. The Department's challenge is to use its

resources wisely and maximize the effectiveness of its programs while meeting or exceeding established performance goals.

3. **Southwest Border Security Issues:** For the second year in a row, the effort to combat organized criminal activities such as the smuggling of humans, drugs, firearms and ammunition, and currency along the 2,000-mile U.S. border with Mexico continues to present a formidable challenge for the Department. The Department's 2011 National Drug Threat Assessment continued to report that crime cartels are primarily responsible for most of the illicit drugs and the thousands of illegal immigrants that are smuggled across the border from Mexico. Simultaneously, firearms and currency are smuggled from the United States into Mexico.

   The Department has responded to these criminal activities with a multi-faceted approach under its Southwest Border Enforcement Initiative, using assets of the Drug Enforcement Administration (DEA), ATF, FBI, the Organized Crime and Drug Enforcement Task Forces (OCDETF), and United States Attorneys' Offices, among others. Major efforts aimed at the Southwest border include ATF's Project Gunrunner; the DEA's El Paso Intelligence Center (EPIC) and its Special Operations Division (SOD); OCDETF co-located strike forces and the multi-agency OCDETF Fusion Center; and the FBI's criminal investigations. However, according to the 2011 National Drug Threat Assessment, the availability of most illegal drugs has continued to increase. While violent crime along the Southwest border as a whole has decreased, as it has nationwide, some locations have seen increases.

   ATF's efforts to manage its Southwest border law enforcement responsibilities have been complicated by allegations that a gun trafficking investigation known as Operation Fast and Furious was mishandled and endangered public safety. Operation Fast and Furious grew out of ATF's Project Gunrunner, a national initiative to stem firearms trafficking to Mexico, and the Department's Southwest Border Enforcement Initiative, which is intended to reduce cross-border drug and firearms trafficking and the high level of violence associated with these activities. The OIG is reviewing the development and implementation of Operation Fast and Furious and similar investigations, including matters such as the involvement of Department components and other law enforcement or government entities in the investigations; information sharing issues among the agencies; the guidelines and other internal controls in place and compliance with those controls during the investigations; and the investigative outcomes.

   In addition to our ongoing review of Operation Fast and Furious, in November 2010 we completed a review of ATF's overall management of Project Gunrunner. Our review found poor coordination and collaboration, and inadequate information sharing between ATF and other Department components, and between ATF and units of the Mexican government. In response to the OIG's 15 recommendations, ATF has reported to the OIG that it will implement a revised Cartel Strategy for combating firearms trafficking, increase its dissemination of intelligence information to its Mexican partners, increase coordination with the Department of Homeland Security's (DHS) Customs and Border Protection and Immigration and Customs Enforcement, and improve its coordination with the DEA. The OIG continues to monitor ATF's implementation of the corrective actions it agreed to take in response to our recommendations.

The OIG also continues to examine other aspects of the Department's Southwest Border Enforcement Initiative. In response to the recommendations we made in our June 2010 report regarding the DEA's El Paso Intelligence Center, the Department has implemented initiatives to improve its operations, including establishing a Predictive Analysis and Targeting Unit to enhance analysis of information regarding drug seizures and the use of fraudulent documents. The DEA also reported to the OIG that it received Office of National Drug Control Policy funding for a program that allowed EPIC to increase drug seizure data reporting into the National Seizure System and, thus, to create a more complete record of drug seizure information. In addition, the DEA reported that EPIC added a Community of Interest feature to its web portal, which provides broader and more interactive sharing of Southwest border information for EPIC's users. With the integration of the Border Intelligence Fusion Section, another new DHS-led organization based at EPIC, the Department may be able to provide more timely and accurate information and analysis to other agencies and intelligence centers.

Border security issues are also affected by the enforcement of immigration laws. Although DHS organizations are charged with most immigration-related responsibilities, we are reviewing the efforts of the Department's Executive Office for Immigration Review (EOIR) to address its backlog of cases.

Although the Department is actively working with other federal agencies, with state and local law enforcement, and with Mexico to respond to the law enforcement challenges along the Southwest border, much remains to be done. The Department's challenge is to continue its efforts to reduce the flow of illegal immigrants, drugs, and weapons between Mexico and the United States effectively, without endangering public safety.

4. **Protecting Civil Rights and Civil Liberties:** While the Department must aggressively continue to pursue its counterterrorism and criminal law enforcement responsibilities, it also must not waver from its commitment and responsibility to uphold civil and constitutional rights. As several of our recent reviews have demonstrated, finding the appropriate balance between these important goals presents a significant challenge.

   The OIG has conducted a series of reviews to evaluate the Department's and the FBI's use of various counterterrorism investigative tools. For example, the OIG is currently conducting its third examination of the FBI's use of National Security Letters (NSL), which are used to obtain information such as telephone and financial records from third parties without a court order. Of particular note, this review will evaluate the automated system the FBI implemented to generate and track NSLs. This system, which the FBI created in response to deficiencies identified in our prior reports, is critical to the responsible administration of the FBI's counterterrorism tools. We are also examining the FBI's use of its authority pursuant to Section 215 of the *USA PATRIOT Act* (Patriot Act) to obtain business records and the FBI's use of its pen register and trap-and-trace authority under the *Foreign Intelligence Surveillance Act.*

   Another powerful investigative mechanism with important implications for civil rights and liberties is the material witness warrant. These warrants are governed by a statute that permits the arrest and detention of witnesses, under specified circumstances and without a showing of probable cause, so that they are available to

provide testimony in criminal proceedings. The OIG has initiated a review of allegations of civil rights and civil liberties abuses in the Department's post-September 11 use of material witness warrants in the national security context.

The Department has also been granted intelligence-gathering authorities under Section 702 of the *FISA Amendments Act of 2008*(FAA) that are useful to its counterterrorism mission but also have civil rights and liberties implications. Section 702 authorizes targeting non-U.S. persons reasonably believed to be outside the United States in order to acquire foreign intelligence information. The OIG is examining the FBI's use of this statute, including the FBI's compliance with targeting and minimization procedures required under the FAA that are designed to ensure that the Department strikes an appropriate balance between its national security responsibilities and its responsibility to protect civil rights and liberties.

With regard to non-terrorism investigations, the Department has made progress implementing recommendations we made in our 2010 report concerning allegations that the FBI improperly targeted certain domestic advocacy groups for scrutiny based upon the exercise of their First Amendment rights. For example, the FBI has reported that its Office of General Counsel has issued instructions to its personnel not to retain information regarding an individual's exercise of First Amendment rights without the requisite law enforcement nexus, statutory authorization, or the individual's consent, and it is developing a corporate policy to the same effect. The FBI has also promised to ensure that FBI agents must 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 members of advocacy groups for activities connected to the exercise of their First Amendment rights. The FBI has not, however, taken the same action with regard to investigation of advocacy groups themselves, and we believe the FBI should do so promptly.

Protecting civil rights and liberties, however, is not just a matter of balancing the citizenry's rights against the need for aggressive law enforcement or counterterrorism investigations. The Department also must ensure that it is properly enforcing civil rights laws. The OIG has undertaken a review of the enforcement of civil rights laws by the Voting Section of the Department's Civil Rights Division. The review is examining the types of cases brought by the Voting Section and any changes in the types of cases over time; any changes in Voting Section enforcement policies or procedures over time; 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.

Another critical challenge facing the Department in protecting civil rights and liberties is ensuring that it has adequate measures in place so that it does not wrongly accuse someone of committing a crime. This issue was raised in the OIG's June 2011 follow-up report examining the FBI's progress in implementing recommendations for improvements to the FBI Laboratory's latent fingerprint operations following the misidentification of Brandon Mayfield in 2004. Mayfield, who was an attorney in Portland, Oregon, at the time, was arrested after the FBI Laboratory examiners wrongly identified his fingerprint as matching a fingerprint found on a bag of detonators connected to the March 2004 terrorist attack on commuter trains in Madrid, Spain. Our follow-up report concluded that the FBI Laboratory has made significant improvements to its latent print operations since the misidentification,

including undertaking research to develop objective criteria for latent fingerprint analysis and substantially revising its Standard Operating Procedures and training materials to address many of the causes of the Mayfield misidentification.

Finally, the Department's responsibility to protect civil rights and liberties includes ensuring the integrity of our justice system in all respects, even after conviction. The Department's challenges relating to detention and incarceration, a crucial aspect of protecting civil rights and liberties, are discussed in the *Detention and Incarceration* section of this document.

5. **Information Technology Systems Planning, Implementation, and Security:** The Department's management of its information technology (IT) systems continues to remain a top management challenge, and it has proven particularly difficult recently. Large IT projects have failed, been delayed, or faced cost overruns just as federal budgets are tightening and cyber intrusions are emerging as a bigger threat. The Department's struggles in planning and implementing IT systems are so serious that in 2010, three Department projects were identified by the Office of Management and Budget (OMB) as "high risk": the Justice Management Division's Litigation Case Management System (LCMS), the FBI's Sentinel case management project, and the FBI's Next Generation Identification (NGI) project to share fingerprint and other biometric information. Since that time, the Department has decided to terminate the LCMS project, after spending millions of dollars on the project. As a result, the Department still struggles with decentralized, disparate litigation case management processes.

   The FBI is continuing with its two projects that OMB identified as high-risk. One is the ongoing development and implementation of the Sentinel project intended to upgrade the FBI's electronic case management system and provide the FBI with an automated workflow process. In our October 2010 report on Sentinel, we expressed our concerns that the implementation of Sentinel had been delayed and was over budget. We found that the deployment of Sentinel's Phase 2 in July 2010 had resulted in some improvements to the FBI's case management system, but it did not deliver much of the functionality that was originally intended. We are currently concluding our eighth review of the Sentinel program, and we continue to have concerns regarding its implementation. When we began this review, the Sentinel project was at a crossroads and the FBI had announced a plan to complete the remaining two phases of Sentinel using a new "Agile development" strategy. We are currently examining the effectiveness of the new Agile strategy and whether the FBI will meet the functionality requirements of the case management system. In addition, we are evaluating the milestones the FBI has set to determine if the FBI will meet its goals without cost overruns.

   Another difficult and costly IT project for the FBI has been the development of NGI, its fingerprint and biometric information sharing project. According to OMB's "Federal IT Dashboard," NGI is expected to cost $1.2 billion by the time it is completed in FY 2017. One of the key challenges for this project is to contain its cost while implementing a design that can accommodate new types of biometric evidence as it becomes available.

   In addition to the three IT systems OMB identified as "high risk," we are concerned about the implementation and maintenance of the Department's Unified Financial Management System (UFMS). The Department has long sought to implement a

Department-wide financial management system to replace the disparate accounting systems used throughout the Department. The OIG reviewed whether the UFMS project was on budget and being implemented according to schedule. In our June 2011 report, we found that although 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, different and sometimes outdated versions of UFMS are in use. Using different and outdated versions of UFMS increases the risk and complexity of making any necessary changes or updates to the system. The significant challenges the Department continues to face regarding the implementation of UFMS include justifying and obtaining sufficient funding for the project in difficult budget times, staff turnover, and ensuring progress while competing with other Departmental priorities. Additionally, the Department must manage and support current UFMS users. Despite the Department's difficulties with UFMS, it is vital for the Department to obtain accurate, near real-time financial information concerning its operations in order to more effectively support its mission.

Another complex and problematic technology project for the Department is the development and implementation of a secure, interoperable, nationwide wireless integrated network to facilitate communication among federal law enforcement officials in different agencies and to meet mandates to use radio frequencies more efficiently. For the past several years, the Department has been attempting to fully implement this project along with the Departments of Homeland Security and the Treasury. In our 2007 report, we noted that the program was at a high risk for failure because of inconsistent funding and weaknesses in the program's governing structure. We continue to have concerns about the program's implementation, and our review of the program is ongoing.

While the Department has had difficulties developing and implementing new systems, it has had some success in making its existing IT systems more secure. The Justice Security Operations Center (JSOC) was established in 2007 to protect Department IT environments from cyber intrusions, incidents, attacks, and espionage. JSOC provides incident response planning, training, and assistance to all Department components and works with components to prevent, monitor, mitigate, and resolve cyber incidents and attacks on the Department. JSOC also coordinates with the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) in reporting incidents. Our audit of the Justice Security Operations Center's capabilities and coordination determined that for the most part, JSOC has been able to effectively monitor network traffic, process the information it receives from Department components and offices, and report incidents to US-CERT. However, we also found that JSOC could further enhance its communication regarding cyber incidents with Department components.

Up-to-date and secure systems are vital to effective management of all of the Department's operations. Developing, implementing, and securing IT systems is a complex, costly, and constantly evolving challenge. Particularly in this era of budget tightening, the Department must ensure that it implements and supports valuable and cost-effective IT systems.

6. **Criminal Law Enforcement:** Although the Department has consistently identified the fight against terrorism as its top priority in recent years, the Department's criminal law enforcement efforts are a major part of its

responsibilities. Transnational organized crime, which encompasses a broad spectrum of criminal activities ranging from illegal gambling to the distribution of illegal drugs and weapons, human trafficking, and financial crimes, is truly global in nature and scope as technological advances enable criminal organizations to operate anywhere in the world. Cyber crime, the use of computers to conduct a wide variety of criminal activities, including fraud, identity theft, and sexual exploitation of minors, is a persistent law enforcement challenge. Fighting violent, transnational, and cyber crime presents an unrelenting management challenge for the Department.

However, there was positive news in the September 2011 report issued by the Bureau of Justice Statistics, which stated that the rate of violent crime committed against U.S. residents aged 12 or older during 2010 fell by 13 percent. Statistics in the FBI's Uniform Crime Report also indicate that crime during 2010 generally decreased 6 percent from 2009 levels, and in particular, the estimated number of violent crimes, such as murder, non-negligent manslaughter, rape, robbery, and aggravated assault, declined for the fourth consecutive year.

Some additional positive news is that the FBI has eliminated the backlog in processing DNA samples of convicted offenders, arrestees, and detainees, which assists in identifying and prosecuting violent criminals. Historically, the FBI Laboratory has had a significant backlog of DNA samples to process as a result of federal legislation enacted in the past 10 years that expanded the scope of DNA sample collection from violent offenders to include anyone who commits a federal offense, as well as to non-U.S. citizens detained in the United States. Our 2011 audit report examining the FBI's efforts to reduce its backlog revealed that the FBI has effectively eliminated its backlog and currently has a manageable monthly workload. However, we identified some areas for improvement, such as the lack of written policies and reporting methods designed to ensure workload levels are accurately identified and reported to management, and the need for better long-term storage of DNA samples, which are maintained indefinitely in the event the FBI must retest a sample to confirm a match.

While the FBI has eliminated the backlog in processing DNA samples of convicted offenders, arrestees, and detainees, it is also responsible for processing forensic DNA collected from crime scenes and evidentiary items such as envelopes, clothing, and drinking glasses, which is then compared to samples collected from known persons in an attempt to identify the perpetrator of a crime. Our August 2010 report examining the FBI Laboratory's forensic DNA case backlog concluded that the FBI Laboratory had a significant and growing backlog of cases requiring the processing of forensic DNA samples, and in September 2011, the OIG initiated a follow-up review to determine if the FBI has made progress to reduce this backlog.

Along with continuing the Department's efforts to reduce the threat, incidence, and prevalence of violent crime generally, dismantling and disrupting organizations that distribute and traffic illegal drugs and firearms continues to present a significant challenge to the Department. According to the Department's 2011 National Drug Threat Assessment, major transnational criminal organizations are largely responsible for the supply of illicit drugs smuggled to the United States, and criminal gangs remain in control of most of the retail distribution of illegal drugs throughout the United States. The study also determined that the threat posed by gang involvement, particularly in the Southwest region of the United States, is increasing. One of the measures the Department has taken to combat this threat is

the creation of the Organized Crime and Gang Section in the Criminal Division. In a review completed in late 2009, we raised serious concerns about the lack of information sharing between National Gang Intelligence Center (NGIC) and the National Gang Targeting, Enforcement, and Coordination Center (GangTECC). In response to our review, in late 2010, the Organized Crime and Gang Section merged with GangTECC. We believe this important step could enhance the Department's efforts to more effectively battle organized crime related to illegal drug trafficking.

However, one of the fastest growing gang-related drug threats is the manufacturing and distribution of methamphetamine, along with the distribution of cocaine and crack cocaine. In 2010, the OIG issued a report describing its review of the DEA's Mobile Enforcement Team (MET) program, which was established primarily to assist local law enforcement agencies in rural areas to reduce drug-related violence and disrupt or dismantle methamphetamine traffickers and laboratories. We determined that a significant problem with the MET program was that it was not deployed in the rural areas for which it was intended. Although the DEA concurred with our recommendations regarding the implementation of the METs, in October 2011, the Department announced that it would eliminate the MET program and reassign 145 positions. The manufacture and distribution of methamphetamine remains a significant problem, and the DEA will have to redirect its efforts to ensure that the elimination of the MET program does not increase the growth of this threat.

In addition to illegal drugs, the use and distribution of illegal weapons is a continuing threat. ATF is responsible for the federal firearms licensee inspection program, which helps ensure that licensed gun dealers do not sell firearms to individuals who are prohibited from owning them. The OIG is conducting a follow-up review of ATF's inspection program, which will evaluate the changes ATF has made to its inspection process, the process it uses to refer suspected criminal violations, and how it institutes administrative actions against licensed dealers who violate federal firearms laws and regulations.

Illegal weapons and drugs, and the violence associated with the manufacture and distribution of illegal drugs, are not the only serious criminal law enforcement threats the Department must address. As sophisticated criminal organizations increasingly take advantage of technological advancements and create online global networks to carry out criminal activity, organized crime has evolved from extortion and intimidation to additionally encompass matters as complex as financial fraud and human smuggling. Organized crime has now truly become "transnational" in scope, and the Department must use sophisticated and aggressive techniques to address it.

Fighting transnational and cyber crime, such as identity theft, remains an important challenge for the Department. Large-scale breaches of corporate and government data networks resulting in the theft of millions of credit and debit card numbers and other personal information have been the subject of numerous recent news articles, underscoring the increase in and prevalence of cyber crime. In April 2011, the Department announced that it had disabled an international "botnet," which infected more than 2 million computers with a malicious software program that enabled criminals to remotely control computers to steal private personal and financial information from unsuspecting users. While the Department made strides in investigating and prosecuting cyber criminals in 2011, it must continue to focus its efforts in this area in conjunction with other law enforcement partners, not the least

because, as we noted in the *Counterterrorism* challenge, cyber intrusion poses a grave threat to national security.

In sum, while the Department has made some progress in the struggle to reduce violent crime, it still faces significant challenges in reducing the global influence of transnational criminal networks.

7. **Restoring Confidence in the Department:** We have reported this as a management challenge since 2007 in response to the controversy surrounding the firing of nine U.S. Attorneys and the hiring of certain career attorneys based on improper political and ideological affiliation. Since we first reported this challenge, we recognize that the Department has undertaken significant efforts toward restoring confidence in the Department. However, as we reported last year, some concerns remain over whether the Department has an adequate disciplinary process for its attorneys and law enforcement personnel, and new issues have arisen concerning enforcement decisions by the Department.

   In 2008 and 2009, the OIG and the Department's Office of Professional Responsibility issued a series of three reports substantiating allegations that Department officials improperly used political and ideological considerations to make employment decisions for career attorney positions in the Civil Rights Division, the Department's Honors Program and Summer Law Intern Program, and other career attorney positions. Since those reports were issued, the Department has addressed most of our recommendations by developing new policies, briefings, and training materials that explicitly instruct hiring officials to use merit-based principles rather than ideological or political affiliation when hiring for career positions. However, a May 2011 Equal Employment Opportunity (EEO) policy that prohibits discrimination on the basis of political affiliation, among other factors, does not specifically state that it applies to detailee positions, not even detailees in policy-making positions. We do not believe that the Department's new EEO policy sufficiently addresses the concerns we raised in one of our hiring reports, and we believe that the Department should provide guidance that includes examples of the types of questions permissible in detailee interviews that are consistent with the Department's policy prohibiting the consideration of political affiliation.

   Law enforcement agency misuse of investigative authority also undermines confidence in Department operations. In a 2007 review, the OIG found that the FBI had improperly or illegally used its National Security Letter authority, which is used in terrorism and espionage investigations and permits the FBI to obtain information such as telephone, e-mail, and financial records from third parties without a court order. To address such concerns, the FBI established the Integrity and Compliance Program, modeled on compliance programs in the private sector, to proactively identify and correct weaknesses in policy, training, or other operations that could result in FBI employees violating the law or FBI policy as they conduct their work. Among other measures, the Office of Integrity and Compliance (OIC) has established a compliance helpline that allows FBI employees to report compliance concerns anonymously, promulgated a non-retaliation policy for reporting compliance concerns, and incorporated an explicit compliance element into the performance appraisal plans of FBI employees. We currently are reviewing the Integrity and Compliance Program to evaluate, among other things, where the program is effective at promoting a culture of integrity and ethical compliance throughout the FBI.

We believe the FBI's establishment of the Integrity and Compliance Program is a good beginning, but as the Department's leading law enforcement agency charged with upholding and enforcing all federal criminal laws, the FBI must continue to develop strong measures to reinforce and sustain its integrity. In 2010 we issued a report finding significant abuses and cheating on the examination designed to measure FBI employees' knowledge of the Domestic Investigations and Operations Guide (DIOG), which implements the Attorney General's Guidelines governing FBI domestic operations. Since our report was issued, the FBI's Office of Professional Responsibility has been investigating and adjudicating the individual cases and has imposed a range of discipline, including non-disciplinary counseling, letters of censure, and suspension without pay for a period of time. The FBI is in the process of updating and revising the DIOG and has announced plans for new training and testing focusing on the revisions. While we believe these measures are important, the FBI must also continually ensure that its personnel are fully trained and are able to demonstrate that they take seriously the responsibility to act in accordance with the Constitution, laws, rules, policies, and procedures governing the FBI's investigative activities.

In addition to addressing law enforcement misconduct, the Department must also address allegations of prosecutorial misconduct in a manner that promotes public confidence. The Department has recently undertaken several measures to address the issue of prosecutorial misconduct. In addition to mandatory training it began in 2010 regarding the government's discovery obligations in criminal cases, the Department has instituted changes to its internal process for investigating, reporting, and addressing prosecutorial misconduct. In 2011, as part of an effort to address allegations that its investigations were not concluded in a timely fashion, a new management team in the Department's Office of Professional Responsibility (OPR) instituted internal management controls and deadlines for completing investigations and reports. Prior backlogs in the publication of OPR's annual report, which describes how it handles its caseload and summarizes its significant investigations, have been eliminated and it is currently up to date. However, the report summaries contained in the annual report provide only limited details regarding the investigations and the basis for OPR's conclusions. While OPR has begun to take steps to determine whether it can make public more information about the cases it investigates, it states that constraints in the provisions of *the Privacy Act* limit the amount of information it can publicly disclose.

In order to facilitate timely and consistent resolution of disciplinary matters arising out of findings of professional misconduct by OPR, the Attorney General also established the Professional Misconduct Review Unit (PMRU) in 2011. The PMRU was designed to reduce delays in imposing attorney discipline and to establish consistent resolution of similar misconduct matters. Beginning in October 2011, the PMRU has been required to submit a report to the Deputy Attorney General semiannually, detailing its compliance with the deadlines established for deciding appropriate disciplinary action. We believe OPR's efforts and the establishment of the PMRU are improvements to the process of addressing prosecutorial misconduct in a more timely and consistent way, but we believe OPR and the PMRU should devise ways to make public more of their findings in order to deter potential misconduct and to promote the Department's efforts to address it.

In addition, as discussed in the *Southwest Border Security Issues* challenge, we are reviewing ATF's gun trafficking investigation known as Fast and Furious and

allegations that it was mishandled and endangered public safety. This review is examining the involvement in and oversight and management of the investigation by multiple Department components, including ATF, the United States Attorney's Office, and divisions within the Department.

Overall, the Department has taken several significant steps toward restoring its reputation for impartiality and excellence, but we believe the Department as a whole should continue to enhance its training and ethics programs and develop ways to make its disciplinary findings more transparent.

8. **Financial Enforcement:** It is especially important in this era of budget cuts and deficit reduction for the Department to vigorously enforce laws related to financial crimes such as mortgage fraud and fraud related to government contracts. In November 2009, President Obama established the Financial Fraud Enforcement Task Force (FFETF) to enhance effectiveness in sharing information among federal, state, and local government agencies to help prevent and combat financial fraud. We believe that this effort is essential and that the Department's role in it is central, but the Department should aggressively pursue financial crimes of all kinds, both independent from and in cooperation with the FFETF. The Department should also continue to pursue civil enforcement actions against those who commit fraud.

   Mortgage fraud has become pervasive, causing the mortgage lending industry, homeowners, businesses, and the national economy to lose billions of dollars annually. The FBI's 2010 Mortgage Fraud Report noted that mortgage fraud continued to steadily increase over 2009 levels. Combating mortgage fraud effectively requires the cooperation of law enforcement, prosecutors, and industry entities. The Department's Mortgage Fraud Working Group, which consists of representatives from the federal inspectors general community, the FBI, U.S. Attorneys' Offices, and the National Association of Attorneys General, helps direct the resources aimed at addressing the growing problem of mortgage fraud. The OIG is performing an audit of the Department's efforts to address mortgage fraud, which will include an assessment of the Department's efforts in and as a result of the Mortgage Fraud Working Group.

   In addition to prosecuting mortgage fraud, the Department recovers significant civil penalties pursuant to statutes such as the *False Claims Act,* which imposes liability upon individuals and organizations that submit fraudulent claims to the government. In October 2011, the Department announced that its total recoveries in *False Claims Act* cases since January 2009 exceeded $7.8 billion.

   However, fraud and mismanagement among recipients of federal funds also demands swift and effective action, and the Department should take steps to ensure that it uses all of the tools at its disposal to protect the funds it administers. For example, the Department should suspend or debar irresponsible recipients of federal financial and nonfinancial assistance and benefits. Suspension and debarment prevent irresponsible recipients from receiving federal funding if they have a criminal conviction or have been indicted for a criminal offense or a willful failure to perform to the terms of a contract or grant. In October 2011, the OIG issued a report regarding the Department's implementation and oversight of debarment and administrative suspension and other enforcement tools. We found that Department awarding officials have generally complied with federal regulations. However, we also found that the Department did not have a formal system to track the status of

suspension and debarment referrals, and that 77 contracts and contract modifications totaling $15 million were awarded to 6 separate suspended or debarred parties. We provided eight recommendations to improve the effectiveness of the Department's suspension and debarment program. The Department already has implemented many of the recommendations we made in our report, such as creating a case tracking system, and it is working to address the remaining recommendations.

The Department's financial responsibilities also include seizing and forfeiting assets criminals and their organizations have acquired through such serious offenses as drug trafficking, human trafficking, white collar crime, and money laundering. In 2011, the OIG issued a report regarding the management and oversight of the United States Marshals Service's Complex Asset Team, which is responsible for helping USMS district offices manage and dispose of unique and complicated assets, such as operating businesses, financial instruments, and commercial real estate holdings. We identified numerous deficiencies, including inadequate record keeping procedures, inadequate pre-seizure planning to ensure that the government can effectively administer a seized asset, and inadequate tracking mechanisms to account for seized assets. In addition, we found that the way the USMS managed complex assets increased the risk that the government could undervalue forfeited assets. The OIG's recommendations included developing and implementing formal procedures regarding the disposition of complex assets, conducting pre-seizure planning, and bolstering the legal, accounting, and valuation knowledge of asset management staff.

The Department must use both criminal prosecution and civil penalty enforcement to ensure that it forcefully exercises its financial enforcement responsibilities. The challenge for the Department is not only to punish those who commit fraud, but also to use all available measures to reduce and deter the incidence of fraud in taxpayer-funded programs.

9. **Detention and Incarceration:** The Department, primarily through the Federal Bureau of Prisons (BOP) and the United States Marshals Service, continues to face the daunting challenge of safely, securely, and economically handling the growing population of federal inmates and detainees. This challenge is multi-faceted, as the BOP must address overcrowding and the resulting higher inmate-to-staff ratios; provide health care, jobs, training, and other rehabilitative programs for inmates while they are incarcerated; and manage residential reentry centers for inmates readjusting to their communities. At the same time, the BOP must effectively manage its own staff to prevent misconduct such as staff smuggling in contraband or staff sexual abuse of inmates. Further, the BOP must constantly work to maintain the infrastructure of its aging facilities.

   Detention and incarceration remains a challenge because the federal inmate population continues to rise. In FY 2011, the federal inmate population increased by 3.6 percent, from 210,227 to 217,768 inmates. This continues the trend of the last decade, which saw the federal inmate population rise by 39 percent since end of FY 2001. This sustained influx of prisoners has led to increased overcrowding across the federal prison system as capacity has not expanded along with the inmate population. As of the end of FY 2011, BOP facilities were filled to 39 percent above rated capacity, as compared with being filled to 32 percent over rated capacity a decade ago. The greatest growth is in the numbers of medium- and high-security

inmates who must be housed in BOP facilities rather than in contract facilities such as local jails. Consequently, the BOP must either add beds to existing BOP institutions, often by converting program or recreational space, or it must build new institutions, which becomes increasingly difficult to finance in an era of budget reductions. Since FY 2006, the Department has identified prison overcrowding as a programmatic material weakness in the Department's annual Performance and Accountability reports.

One way to assist in reducing the inmate population is through the International Prisoner Treaty Transfer Program, which permits certain foreign national inmates from treaty nations to transfer to their home countries to serve the remainder of their sentences. The OIG is currently reviewing the responsibilities of the Bureau of Prisons and the Criminal Division's International Prisoner Transfer Unit in the treaty transfer program.

The increasing inmate population also challenges the BOP's ability to manage its workforce and maintain a safe and secure prison environment. The BOP's staffing has not increased commensurately with the inmate population. From FY 2001 to FY 2011, the inmate-to-staff ratio increased from 4.1 inmates for each correctional officer to 4.94 to 1, an almost 21-percent increase. According to the BOP, increases in prison crowding and the inmate-to-staff ratio are correlated with increases in inmate violence. The stretching of the BOP workforce also increases the challenge for the BOP to detect and prevent misconduct by staff members. The number of misconduct investigations of BOP Correctional Officers doubled from FY 2001 to FY 2010, from 2,299 to 4,603. Arrests of Correctional Officers also increased, as a total of 272 Correctional Officers were arrested, increasing 89 percent from 18 in FY 2001 to 34 in FY 2010. Although the number of BOP employees involved in misconduct is only a fraction of the BOP's workforce of over 38,000, misconduct by even a few employees can undermine the safety and security of institutions and violate the rights of inmates.

We believe the BOP can help prevent staff misconduct by screening out unsuitable applicants when hiring correctional officers and staff members. In September 2011, the OIG released a report analyzing whether the BOP's hiring process could more effectively identify potentially unsuitable applicants for Correctional Officer positions. Through logistic regression analysis, we found that combinations of certain applicant characteristics have strong relationships with an increased likelihood that substantiated misconduct resulting in at least a 1-day suspension would occur during the first 2 years after a Correctional Officer begins work. We determined that if the BOP were to systematically evaluate individuals based on combinations of factors in addition to the single thresholds it now relies on, it could add a useful tool to its screening practices. The BOP agreed to examine how it might implement this approach.

Along with preventing staff misconduct generally, another especially serious issue is preventing sexual abuse of inmates. The *Prison Rape Elimination Act of 2003* mandated that the Department review proposed standards issued by the National Prison Rape Elimination Commission and issue national standards to enhance the detection, prevention, reduction, and punishment of prison rape by June 2010. The Department did not meet that deadline until January 24, 2011, when it released a proposed rule designed to prevent and respond to sexual abuse in

incarceration settings. The Department plans to issue the final rule by December 2011, according to the schedule it published in the *Federal Register.*

In addition to the formidable challenges it faces in eliminating staff misconduct, the BOP also faces challenges in supporting the effective and safe operation of its prisoner work program, Federal Prison Industries, Inc. (FPI), a wholly owned federal government corporation that operates under the trade name UNICOR. Created by Congress in 1934, FPI's mission is to provide employment and training to keep federal inmates productively and safely occupied. At the same time, FPI's mandate is to maintain its self-sufficiency through the sale of its products and services. However, over the last 2 fiscal years, FPI closed or downsized 40 of its 109 work facilities and reduced the number of inmates working in FPI facilities so that, although FPI has a goal of employing 25 percent of work-eligible inmates, at present it employs only about 9 percent. The OIG is currently reviewing FPI's business management practices.

Aspects of the Department's *Detention and Incarceration* challenge also extend to the United States Marshals Service, which is responsible for maintaining the safety of tens of thousands of detainees awaiting trial or sentencing. The primary difficulty the USMS faces is to arrange for safe, affordable, and cost-effective detention space to house some 60,000 federal detainees, 80 percent of whom must be housed in state and local jails or other community detention facilities because there is insufficient federal space in which to house them. As discussed in more detail in the *Implementing Cost Savings and Efficiencie**s*** challenge, housing detainees in a safe environment in a cost-effective manner continues to represent a significant challenge for the Department, and the USMS must ensure that such facilities are not in a position to take advantage of the need for space by charging unjustifiable rates.

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

10. **Grants and Contract Management:** The Department's management of grants and contracts it awards has long presented a challenge in light of the large amounts of money at stake. Since FY 2009, the Department has received over $15 billion in grant funds to award through the combined appropriations from the regular appropriations cycle and pursuant to the *American Recovery and Reinvestment Act of 2009* (Recovery Act). In addition, the Department also spends a sizable amount through contract purchases each year. According to USAspending.gov, the Department awarded approximately $6.3 billion in contracts for goods and services for FY 2011. In light of this large volume of grant and contract awards, the OIG devotes considerable attention through audits and fraud investigations to overseeing the Department's efforts at grants and contract management. While we believe the Department has made concerted efforts to enhance its management of its responsibilities, such as increasing training and providing assistance in determining how to collect performance information, these changes will take time to fully implement and to incorporate into the Department's regular practices.

Through FY 2011, the Department has obligated more than 99 percent of its Recovery Act funds, and the grantees have received approximately 72 percent of the Recovery Funds that have been obligated. Such significant amounts of money

require strict controls over the way the funds are awarded and spent. The Department has taken significant steps in recent years to improve its grant management practices, including implementing better controls to ensure that it correctly ranks applications, treats applicants consistently, documents award decisions, and resolves conflicts of interest. While the Department has implemented corrective actions to address the majority of the concerns we have raised in our reports, some recommendations remain open. For example, the Office on Violence Against Women (OVW) revised its Peer Review Guidelines to ensure that peer reviewers carefully assess applications for potential conflicts of interest before they actually evaluate and score the applications. However, the revised guidelines do not provide staff with a process to follow when conducting an internal review that will check for scoring errors and verify the accuracy of future final peer review scores. We believe that OVW should provide specific guidance as to the correct protocols necessary for an internal review. In addition, our February 2011 review of the award process for the Bureau of Justice Assistance's (BJA) Recovery Act Correctional Facilities on Tribal Lands Grant Program revealed that an internal BJA peer reviewer had significant involvement with an applicant that received an award. Specifically, the peer reviewer had participated in the applicant's Advisory Committee, but the reviewer still certified that he had no conflicts of interest while reviewing program applications. We believe that the BIA should consider strengthening internal controls to reduce the risk of appearances of conflicts of interest or favoritism towards a particular grantee.

One of the most significant challenges remaining for the Department in this area is to translate improvements it has made in its own management of grants into improvements in grantees' management of funds. The Department must improve its oversight of grantees' internal controls to ensure funds are being spent in accordance with the terms of the grants. For example, the Office of Justice Programs (OJP), the Department's primary grant awarding agency, provides grants to state and local law enforcement and community organizations to prevent and control crime, improve the criminal and juvenile justice systems, increase knowledge about crime and related issues, and assist crime victims. The OIG recently reviewed OJP's monitoring and oversight of grants it awarded in FYs 2009 and 2010. During that period, OJP made over 13,000 grant awards totaling more than $7.7 billion, which included over 4,000 Recovery Act grants, totaling about $2.8 billion. Our March 2011 report noted that while OJP has significantly improved its monitoring and oversight, it should make additional improvements such as more thoroughly assessing and documenting how it reviews the programmatic, financial, and administrative aspects of the grants it awards and more clearly describing the methodology it uses to select which grants to monitor. We also recommended that the Department eliminate duplication among certain grant monitoring services performed by OJP, OVW, and the Community Oriented Policing Services Office.

The Department's limited budgetary resources also currently present a considerable challenge to its efforts to improve oversight of grantees' internal controls. In April 2011, budget restrictions forced OJP to freeze most travel, including travel for monitoring, grantee training, programmatic conferences, and other programmatic travel. It remains to be seen whether OJP's alternative monitoring plans, which include multi-office site visits, local travel, and remote monitoring (enhanced desk reviews), will slow or decrease the progress it has made in enhancing its oversight efforts.

Further, while monitoring and oversight of grants is an important responsibility, we also believe that the Department must take further action to address outstanding recommendations to remedy questioned costs from our audits of grantees. We understand that corrective actions take time to implement. However, some recommendations have been outstanding for more than 6 years and involve potentially significant amounts of money. For example, in a December 2006 report of our audit of the Department's grant closeout process, we identified over $37 million in questioned costs related to drawdowns occurring more than 90 days past the grant end date. Effective oversight and monitoring includes follow up to ensure that taxpayer dollars have been spent in accordance with grant requirements.

In addition to grants, the Department spends a considerable amount of taxpayer funds in its contracts for goods and services. All government agencies are required to promote full and open competition for these contracts, which is critical to ensure that the government receives the best offer for goods and services that it procures. One of the key steps in the procurement process is thoroughly evaluating the vendors' technical proposals to determine which vendors have met the minimum requirements of the request for proposal and have the most effective plan for accomplishing those requirements. The failure to undertake this evaluation can have significant adverse consequences. For example, we reviewed the United States Marshals Service's oversight of its Judicial Facilities Security Program. Our November 2010 report found that the USMS awarded a contract worth approximately $300 million to a court security officer contractor with a history of fraudulent activities, despite an earlier fraud alert issued by the OIG's Investigations Division. The contractor ultimately filed for bankruptcy, leaving many court security officers temporarily without payment for their services.

Some of the largest contracts that the Department awards are related to the planning and implementation of complex information technology systems. As previously discussed in *Information Technology Systems Planning, Implementation, and Security,* the management and oversight of IT contracts to minimize cost overruns and provide planned system functionality remain a top challenge for the Department.

In sum, the Department expends a considerable amount of scarce resources on grants and contracts. It is essential that the Department use proper controls to ensure grants and contracts are properly awarded and monitored to eliminate waste, fraud, and abuse.