Section IV

Management Section
(Unaudited)

Overview

Each year, the Department identifies existing and potential management challenges, weaknesses, and areas in need of improvement. Two primary sources used to identify these issues are the Department's OIG-identified Top Management and Performance Challenges and the Federal Managers' Financial Integrity Act (FMFIA) assessment process. The challenges identified by the Department's OIG are from an auditor's perspective and include areas of concern that bear significantly on how well the Department carries out its mission and meets its responsibilities as a steward of public funds. The FMFIA assessment process evaluates the effectiveness of internal controls to support effective and efficient programmatic operations, reliable financial reporting, and compliance with applicable laws and regulations (FMFIA § 2) and whether financial management systems conform to financial system requirements (FMFIA § 4).

Presented on the following pages are the OIG-identified Top Management and Performance Challenges in the Department, Department management's response to those challenges, and the Corrective Action Plan resulting from the FMFIA assessment.

This page intentionally left blank.

OIG Top Management and Performance Challenges in the Department of Justice

November 7, 2012

MEMORANDUM FOR THE ATTORNEY GENERAL
THE DEPUTY ATTORNEY GENERAL

FROM: MICHAEL E. HOROWITZ
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) 2012 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.

The challenges are based on the OIG's oversight work, research, and judgment. While the challenges are not presented in priority order, we continue to believe that *Safeguarding National Security* presents the greatest challenge to the Department. We also have highlighted the many challenges the Department faces in enforcing federal law in a coordinated and effective fashion, and we again have highlighted the importance of *Restoring Confidence in the Department*, as recent events – most notably the events detailed in our August 2012 report on the Bureau of Alcohol, Tobacco, Firearms and Explosives' Operation Fast and Furious and Related Matters – have once more placed the Department's role as a custodian of the public's trust under intense scrutiny.

In addition, we have posed many questions that go to the heart of the Department's structure and operations, such as whether the Department is adequately addressing the growing costs of the federal prison system, whether aspects of the Department's four law enforcement components could be further consolidated with each other, and whether the Department's operations duplicate similar efforts by other federal agencies. These questions are not new, but they take on new importance in this era of constrained budgets. Together, these issues pose a clear, if daunting, challenge: the Department must have in place an innovative and transparent strategic vision for how to fulfill its mission without requiring additional resources.

We hope this document will assist the Department 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

This page intentionally left blank.

1. Safeguarding National Security: Terrorism remains a significant threat world-wide as the country moves into the second decade since the terrorist attacks of September 11, 2001. In its latest "Report on Terrorism," the National Counterterrorism Center identified more than 10,000 terrorist attacks world-wide during calendar year 2011, resulting in nearly 45,000 victims and over 12,500 deaths in 70 countries. Consequently, safeguarding national security has remained the Department of Justice's (DOJ or Department) highest priority and the focus of intensive resources: the Federal Bureau of Investigation (FBI) alone dedicated approximately 4,200 of its approximately 13,000 special agents to investigate more than 33,000 national security cases in fiscal year (FY) 2011.

The Office of the Inspector General's (OIG) oversight has consistently demonstrated that the Department faces many challenges in its efforts to help protect the nation from attack. One such challenge is ensuring that national security information is appropriately shared among Department components and the intelligence community so that responsible officials have the information they need to act in a timely and effective manner. The OIG is currently conducting numerous reviews in this area. For example, we are examining whether the FBI and National Security Division are appropriately handling and coordinating the Department's responsibilities with regard to terrorist financing, a crucial component of the country's efforts to disrupt terrorist organizations and prevent future attacks.

The OIG is also continuing its oversight of information sharing and coordination among Department components with respect to watchlisting terrorists. For example, in audits conducted in 2008 and 2009, the OIG concluded that the FBI was not adding known or suspected terrorists to the Terrorist Watchlist maintained by the FBI's Terrorist Screening Center in a timely fashion and that it lacked effective procedures to ensure that names on the watchlist were updated or removed as required by law. We have initiated another review to determine whether the FBI has made progress toward remedying these deficiencies.

We are also reviewing the operations and functions of the FBI's Foreign Terrorist Tracking Task Force, an entity formed to provide information that helps keep foreign terrorists and their supporters out of the United States or leads to their removal, detention, prosecution, or other legal action. Our review is evaluating whether the FBI has implemented a viable strategy to locate and track suspected terrorists and their supporters, including its efforts to coordinate with law enforcement and intelligence agencies both inside and outside the Department, and whether the FBI has appropriately managed terrorist-related information maintained by the task force.

In addition to the challenges of information sharing, the Department faces the challenge of ensuring the appropriate use of the tools available to its personnel responsible for monitoring and detecting national security risks and threats. The importance of this challenge was demonstrated in two prior OIG reviews assessing the FBI's use of national security letters (NSL), which allow the government to obtain information such as telephone and financial records from third parties without a court order, but which are subject to legal requirements that protect fundamental civil liberties and privacy interests. These reviews found that the FBI had misused this authority by failing to comply with important legal requirements designed to protect civil liberties and privacy interests, and we therefore made recommendations to help remedy these failures. The FBI has implemented many of these recommendations and continues to make progress in implementing others. However, some recommendations remain outstanding. We are now conducting our third review of NSLs to assess the FBI's progress in responding to those recommendations and to evaluate the FBI's automated system for tracking NSL-related activities and ensuring compliance with applicable laws. The review will also evaluate the FBI's use of two related national security tools: the authority to obtain business records pursuant to Section 215 of the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act*, and the

authority to use pen register and trap-and-trace devices under the *Foreign Intelligence Surveillance Act* (FISA).

Similarly, the OIG recently completed a review of the Department's use of Section 702 of the *FISA Amendments Act* (FAA), which culminated in a classified report released to the Department and Congress. Section 702 confers authority to "target persons reasonably believed to be located outside the United States to acquire foreign intelligence information." As required by the FAA, the OIG examined the number of disseminated FBI intelligence reports containing 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. The OIG also reviewed the FBI's compliance with the required targeting and minimization procedures.

2. Enhancing Cyber Security: Computer systems that are integral to the infrastructure, economy, and defense of the United States face the constant and rapidly growing threat of cyber intrusion and attack, including the threat of cyber terrorism. According to recent statements by the Secretary of Defense, the United States is increasingly vulnerable to foreign computer hackers seeking to launch cyber-attacks on critical national infrastructure. While the number of cyber security incidents directly affecting the Department remains classified, a recent study by the Government Accountability Office (GAO) found that the number of such incidents reported by federal agencies increased by nearly 680 percent from 2006 to 2011. The Department will continue to face challenges as it seeks to prevent, deter, and respond to cyber security incidents – both those targeting its own networks and those that endanger the many private networks upon which the nation depends.

The Department has identified the investigation of cyber crime and the protection of the nation's network infrastructure as one of its top priorities. The Department's FY 2013 budget request highlights the increased resources sought for the Comprehensive National Cybersecurity Initiative, which is intended to combine the missions of various federal agencies to protect government computer systems and begin to address the protection of private sector systems, as well as for the FBI's cyber terrorism investigations and the forensic examination of digital evidence. The budget request also seeks increased resources for the National Cyber Investigative Joint Task Force (NCIJTF), an FBI-led multi-agency task force to coordinate the counterintelligence, counterterrorism, intelligence, and law enforcement activities of its member organizations in response to cyber threats.

In addition to funding increases, the Department has sought to strengthen cyber security by responding to recommendations made in OIG reports relating to cyber security. For example, in September 2011, the OIG released an audit report examining the operations of the Justice Security Operations Center (JSOC), which was established in 2007 to protect the Department's information technology systems from cyber intrusions, attacks, espionage, and other cyber incidents. The audit identified needed improvements to JSOC's activities, including its cooperation and coordination with Department components and with the Department of Homeland Security's United States Computer Emergency Readiness Team. We made 20 recommendations to improve JSOC's ability to report and manage information pertaining to cyber incidents, and to enhance the effectiveness of coordination between JSOC and components and offices. The Department has implemented corrective action and closed 19 of the 20 recommendations. The Department has also implemented and closed all 10 recommendations in the OIG's 2011 audit report assessing the NCIJTF and the capabilities of FBI field offices to investigate national security cyber intrusion cases.

However, the challenges posed by cyber crime multiply as cyber threats grow in number and complexity. Of central importance to any cyber security strategy is working effectively with the private sector. The Department must not only encourage the private sector to invest in the security of its own networks, but it must also conduct aggressive outreach to assure potential victims of cyber crime that proprietary network information disclosed to law enforcement will not become public. Even a modest increase in the rate at which cyber crimes are reported would afford the Department invaluable opportunities to learn the newest tactics used by an unusually dynamic population of criminals and other adversaries, and to arrest and prosecute more perpetrators.

Cyber intrusion and attack also pose risks to the security of the Department's information, the continuity of its operations, and the effectiveness of its law enforcement and national security efforts, and the Department consequently faces the challenge of protecting its own systems, including systems that protect its sensitive and classified information. Partly in response to the highly publicized 2010 incident in which an Army intelligence analyst allegedly provided classified combat footage and hundreds of thousands of classified State Department documents to a website devoted to publishing secret information, news leaks, and classified media from anonymous sources, the President issued an executive order requiring a government-wide program for deterring, detecting, and mitigating insider threats. As a result, in March 2012 the Department established an Insider Threat Detection and Prevention Working Group. The Department plans to issue a strategy and guidance on how components should implement an insider threat program and to provide training on insider threats.

But more can be done. For example, the OIG annually conducts its *Federal Information Security Management Act* audits, which include testing the effectiveness of information security policies, procedures, and practices of a representative subset of agency systems. The OIG recently reviewed the security programs and a selection of individual systems for six Department components: the FBI, Justice Management Division (JMD), Federal Bureau of Prisons (BOP), U.S. Marshals Service (USMS), Criminal Division, and Tax Division. These audits identified deficiencies that included inadequate configuration management settings that expose workstations to cyber security threats; inadequate identification and authentication controls that increase the risk of inappropriate or unauthorized access to information systems; audit and accountability controls that decrease the timely identification of operational problems and unauthorized activity; and inadequate contingency planning that increases the risk that information systems will not continue to operate during an emergency. In addition, the Civil Division has yet to complete corrective actions in response to the 2009 OIG audit report finding significant vulnerabilities in its laptop computer encryption policies and practices. The Department must strive not only to correct these deficiencies, but to avoid them in the first instance.

3. Managing the Federal Prison System: Housing a continually growing and aging population of federal inmates and detainees is consuming an ever-larger portion of the Department's budget, making safe and secure incarceration increasingly difficult to provide, and threatening to force significant budgetary and programmatic cuts to other DOJ components in the near future. In FY 2006, there were 192,584 inmates in BOP custody. As of October 2012, the BOP reported 218,936 inmates in its custody, an increase of nearly 14 percent. Not surprisingly, these trends mirror the increased number of federal defendants sentenced each year, which rose from approximately 60,000 in FY 2001 to more than 86,000 in FY 2011, according to the U.S. Sentencing Commission.

The Department's own budget reports demonstrate the fundamental financial challenges facing the Department. Fifteen years ago, the BOP's enacted budget was $3.1 billion, which represented approximately 16 percent of the Department's budget. In comparison, the Department has requested

$6.8 billion for the BOP in FY 2013, or 26 percent of the Department's total FY 2013 budget request. Moreover, the President's FY 2013 budget projects the budget authority for federal correctional activities to rise to $7.4 billion by 2017.

The Department has been aware for years of the problems that it is facing due to the rapidly expanding prison population. The Department first identified prison overcrowding as a programmatic material weakness in its FY 2006 Performance and Accountability Report, and it has been similarly identified in every such report since. In fact, prison overcrowding was the Department's only identified material weakness in this last year. To reduce overcrowding in existing federal prisons as the inmate population continues to grow, the BOP has contracted with private sector and state and local facilities to house certain groups of low-security inmates, and it recently purchased an existing state facility. The Department also has expanded existing federal facilities, and the GAO recently reported that from FY 2006 through FY 2011 the BOP increased its rated capacity by approximately 8,300 beds as a result of opening 5 new facilities.

Yet despite this increase in bed space since FY 2006, and despite the growth in BOP budget authority from approximately 22 percent of the DOJ budget in FY 2006 to the requested 26 percent in FY 2013, conditions in the federal prison system continued to decline. Since FY 2000, the BOP's inmate-to-staff ratio has increased from about four-to-one to a projected five-to-one in FY 2013. Since FY 2006, federal prisons have moved from 36 percent over rated capacity to 39 percent over rated capacity in FY 2011, with medium security facilities currently operating at 47 percent over rated capacity and high security facilities operating at 52 percent over rated capacity. Moreover, the Department's own outlook for the federal prison system is bleak: the BOP projects system-wide crowding to exceed 44 percent over rated capacity through 2018. In an era where the Department's overall budget is likely to remain flat or decline, it is readily apparent from these figures that the Department simply cannot solve this challenge by spending more money to operate more federal prisons unless it is prepared to make drastic cuts to other important areas of the Department's operations.

One approach the Department recently has embraced to reduce prison system costs is to focus on reducing recidivism. According to Department figures, of the more than 45,000 federal offenders who leave prison every year and return to American communities, approximately 40 percent are rearrested or have their supervised release revoked within 3 years. The Deputy Attorney General has spoken about various alternatives to incarceration – including the Pretrial Alternatives to Detention Initiative in the Central District of Illinois, the Conviction and Sentence Alternative program in the Central District of California, and the BRIDGE program in the District of South Carolina.

The Department also is pursuing legislative proposals targeting the problem of recidivism. Recent proposals include the *Federal Prisoner Recidivism Reduction Programming Enhancement Act*, which would allow prisoners who successfully participate in programs that have been demonstrated to reduce recidivism to earn up to 60 days per year of credit toward the completion of their sentences, and the *Federal Prisoner Good Conduct Time Act*, which would increase the amount of time a federal prisoner could earn for good behavior to reduce his or her sentence.

The Department's efforts to develop new alternatives to incarceration also may help reduce overcrowding and costs. For example, it supported changes to the federal sentencing guidelines to permit drug or mental health treatment for certain low-level offenders to serve as an alternative to incarceration. It also revised the *U.S. Attorneys' Manual* regarding available alternatives to incarceration, such as pretrial diversion programs that offer addicted defendants treatment and monitoring instead of prosecution.

Additionally, the Department can make better use of existing programs to realize cost savings and reduce overcrowding. For example, in December 2011, the OIG reviewed the Department's 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. According to the U.S. Sentencing Commission, 48 percent of defendants sentenced in FY 2011 were non-U.S. citizens, up from 37 percent in FY 2006, and the BOP reported that, as of August 2012, up to approximately 27 percent of federal inmates were foreign nationals. Yet the OIG review found the BOP and the Criminal Division's International Prisoner Transfer Unit had rejected 97 percent of foreign national inmates' requests to transfer from FY 2005 through FY 2010, and in FY 2010, slightly less than 1 percent of the 40,651 foreign national inmates in the BOP's custody were transferred to their home countries to complete their sentences. While some factors that reduce the number of transfers are beyond the Department's control, the OIG found the Department could take steps to increase the number of inmates transferred and the timeliness of the process that would result in potentially significant savings. The Department is now implementing the OIG's 14 recommendations to manage the program more effectively. Similarly, the OIG is reviewing the BOP's implementation of its Compassionate Release Program, which allows the Department to release prisoners under extraordinary and compelling conditions, such as terminal illness.

Importantly, the challenges facing the BOP and the Department are not limited to overcrowding and rapidly increasing costs. For example, the Department bears the heavy responsibility of preventing the sexual abuse of inmates in BOP facilities and detainees in the custody of the USMS. The OIG raised concerns about this issue in a 2009 report on the Department's efforts to detect and deter staff sexual abuse of inmates in federal prisons, and the *Prison Rape Elimination Act of 2003* (PREA) required the Department to issue by June 2010 national standards to enhance the detection, prevention, reduction, and punishment of prison rape. The Department issued its final rule in May 2012, and the new rule is responsive to the concerns we previously raised. However, the BOP's and USMS's implementation of the rule may prove challenging. Among other requirements, the new standards obligate agencies to include compliance with PREA standards as a requirement in any new contract or contract renewal with outside entities, thus imposing new monitoring obligations on the BOP and USMS with respect to private contract facilities.

The Department also faces challenges in managing its prisoner work program, Federal Prison Industries, Inc. (FPI), a wholly owned federal government corporation created by Congress that operates under the trade name UNICOR. As of September 2012, the FPI had closed 36 of 104 factories while opening only 13 new factories in the previous 5 years, resulting in an overall decrease in both the number of facilities and the number of inmates working in FPI facilities. The FPI is currently employing only about 8 percent of work-eligible inmates, well below its goal of 25 percent. The OIG is reviewing the FPI's business management practices to determine what factors have led to the significant reduction of inmate work and the FPI's plans to maintain and create work opportunities for inmates. Also under review are the FPI's management of its business operations, including development and significant changes to product offerings, and how the FPI is using new legislative authority that would allow it to grow its business and employ more inmates.

4. Leading the Department in an Era of Budget Constraints: The Department's mission has remained substantially unchanged since 2001, yet the budgetary environment in which the Department operates has changed dramatically. From FY 2001 through FY 2011, the Department's discretionary budget grew by more than 41 percent in real dollars, from $20.4 billion to $28.9 billion. Yet the Department's discretionary budget decreased by more than 7 percent in FY 2012 to $26.8 billion, and its FY 2013 discretionary budget request of $26.7 billion represents a further decrease from historical levels. With the President's budget for FY 2013 forecasting additional cuts to the overall Executive Branch discretionary budgets in coming years, it appears

likely that Department leadership faces the significant challenge of fulfilling the Department's mission without the assurance of increased resources.

The Department has taken initial steps to reduce its budget. For example, the Attorney General issued a memorandum ordering a Department-wide temporary hiring freeze and instructed components to limit travel, training, and conference spending. In February 2011, the Deputy Attorney General provided guidance for operational and programmatic efficiencies. The Department has implemented cost-saving initiatives relating to information technology expenditures, travel expenses, and time-and-attendance tracking. The Attorney General also created his Advisory Council for Savings and Efficiencies (SAVE Council) in 2010, which has taken such steps as eliminating the Drug Enforcement Administration's (DEA) Mobile Enforcement Teams, posting administrative notices on the forfeiture.gov website, consolidating Department offices, and merging JMD's strategic planning and management functions.

With respect to the Department's budget request for FY 2013, the Department has proposed almost $700 million in efficiencies, offsets, and rescissions, representing approximately 2.6 percent of the Department's total budget. Approximately $647 million of these cuts resulted from administrative efficiencies, non-grant program reductions, and rescissions of prior year balances. However, the Department also has proposed approximately $228 million in FY 2013 program increases, including: $55 million for investigating and prosecuting financial and mortgage fraud; $32 million for traditional missions (civil rights, cyber security, intellectual property, transnational organized crime, and immigration services); and $141 million to ensure prisoners and detainees are confined in secure facilities and to improve federal prisoner reentry.

As part of the effort to find operational efficiencies, the Department should redouble its efforts to adopt and implement OIG recommendations designed to reduce costs. We understand that corrective actions take time to implement, but as of September 2012, 819 OIG recommendations to the Department remained open, including many recommendations that could lead to substantial cost savings. Our FY 2012 audits and related single audits also identified $25 million in questioned costs that the Department should make every effort to resolve and, if necessary, recover. Additionally, various GAO reports have identified functions that the Department may wish to consolidate, such as the recent report recommending that the Department consider combining its Asset Forfeiture Program with that of the Treasury Department.

The Department must also focus on enhancing long term planning for large information technology projects. For example, in January 2012, the OIG released a follow-up audit report examining the status of the Integrated Wireless Network program intended to address the Department's aging law enforcement communications systems, meet federal law enforcement requirements to communicate across agencies, allow interoperability with state and local law enforcement partners, and meet mandates to use federal radio frequency spectrum more efficiently. Our previous audit had concluded that the program was at high risk of failing to secure an integrated wireless network for use by the Department, the Department of Homeland Security, and the Treasury Department. We found that by 2012, after spending more than $356 million over 10 years, the program had yet to achieve the results intended when the Department began developing it in 1998 due to inconsistent funding from Congress, the departure from the program of a major federal agency partner, and unforeseen changes in the technological environment. Similarly, our September 2012 audit report examining the FBI Laboratory's forensic DNA case backlog found that after spending $14 million since 2003 on two attempts to develop an information management system, the FBI Laboratory did not have a system capable of electronically managing laboratory operations, and a new system was in the preliminary stages of development.

The Department should also continue to strengthen its efforts to collect criminal penalties, civil judgments, and other funds owed to the Department, while also ensuring that enforcement efforts across its components and sub-components remain equally and appropriately vigorous. In FY 2011, the U.S. Attorneys' Offices collected $6.5 billion in criminal and civil actions – $2.7 billion in restitution, criminal fines, and felony assessments, and $3.8 billion in individually and jointly handled civil actions – as well as an additional $1.68 billion collected through asset forfeiture actions in partnership with other divisions and agencies. However, at the end of FY 2011, the U.S. Attorneys' Offices reported an ending principle balance of nearly $75 billion relating to criminal and civil actions that remained uncollected. In addition, collection efforts may vary substantially among the U.S. Attorneys' Offices. For example, according to the United States Attorneys' Annual Statistical Report, a single office accounted for more than 68 percent of the approximately $1.5 billion recovered through civil asset forfeitures during FY 2011. Based on our review of Annual Statistical Reports for other fiscal years, this substantial variance does not appear to be anomalous.

Leading the Department in this climate of budget constraints will require careful budget management and significant improvements to existing operations. Discrete operating efficiencies are unlikely to fully address the significant challenges of moving the Department from an era of expanding budgets into an era of budget constraints without sacrificing its mission. It is therefore incumbent upon the Department to plot a new course for the current budgetary environment, one that streamlines the Department's operations while simultaneously taking on the most important and fundamental questions about how the Department is structured and run.

5. Protecting Civil Rights and Civil Liberties: Protecting civil rights and liberties requires that the Department ensure that it is respecting civil liberties and properly enforcing civil rights laws. The Attorney General has stated that "[s]afeguarding the civil rights of every American is at the heart of what we do, and represents our core mission." Yet this core mission remains a challenge in many respects.

Emerging technology – and shifting rules relating to its use – poses one of the most difficult challenges to the Department's efforts to protect civil rights and liberties, particularly when effective law enforcement techniques have the potential to encroach on civil rights and liberties. For example, in January 2012, the U.S. Supreme Court issued its decision in *United States* v. *Jones*, in which it found that installing a global positioning system (GPS) tracking device on a surveillance target's vehicle constitutes a search under the Fourth Amendment. Overnight, the Court's ruling required prosecuting attorneys to exercise greater oversight of the use of GPS devices and necessitated updated guidance and training with respect to the use of such technology. Subsequently, in August 2012, a federal appeals court held in *United States* v. *Skinner* that users of cellular telephones do not have a reasonable expectation of privacy in the data emanating from a cell phone that show its location. Whether other federal appellate courts will reach the same conclusion cannot be known, thus adding further complexity and uncertainty to the rules governing law enforcement's use of emerging surveillance technologies. The Department will continue to face similar challenges as technologies evolve, and it must be prepared to adapt quickly to a fast-changing landscape of legal rules.

Another emerging technology, unmanned aerial vehicles, or drones, has already joined the arsenal of some U.S. law enforcement agencies, and the Federal Aviation Administration predicts that 30,000 drones will be used in the United States within 20 years. Advances in drone technology represent an obvious opportunity for law enforcement, as drones can be equipped with facial or biometric recognition technology to identify and track individuals, and can even be recharged while in flight using a laser on the ground. The Department provides grant funds to state and local

governments to purchase equipment and technology that could be, and has been, used for surveillance drones. Yet drones also raise significant privacy concerns, and there are several legislative proposals to improve the privacy safeguards attached to their use. As the use of drones increases, the Department will face the challenge of monitoring the use of its grant money to ensure that drone technology purchased with federal funds is used in a manner consistent with applicable privacy and civil rights protections.

Abolishing unlawful discrimination is one of the most important facets of the Department's civil rights and liberties mission. To that end, the Department's Civil Rights Division works to uphold the civil and constitutional rights of all Americans by enforcing federal statutes prohibiting improper discrimination with regard to criminal enforcement, disability rights, educational opportunities, employment, and housing. To ensure that this important work is conducted in an evenhanded manner, the OIG is conducting a review of the Civil Rights Division's Voting Section. Our 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. We are also investigating allegations that Voting Section managers improperly took political affiliations into account in hiring lateral attorneys and gave preferential treatment to political allies in responding to FOIA requests.

Finally, the OIG's recent investigation into the Bureau of Alcohol, Tobacco, Firearms and Explosives' (ATF) Operation Fast and Furious raised concerns about the approval process involving one of the Department's most intrusive investigatory tools, the wiretap. During our review, we determined that at least three of the five Deputy Assistant Attorneys General who reviewed the wiretap applications regularly relied on summary memoranda provided by subordinates when approving such applications rather than undertaking a personal review of the applications themselves. Given the significant intrusion on individual liberties that occurs following the approval of a wiretap application, as well as the substantial limitations that Congress placed on the approval of a wiretap, we concluded that the Department needed to strengthen its approval process and made a recommendation for it to do so.

6. Restoring Confidence: The Department must address several substantial challenges to ensure that it strengthens and maintains the public's trust in its fairness, integrity, and efficiency.

Inadequate management and oversight of law enforcement activities undermine confidence in Department operations. Over the past year, significant public attention has focused on ATF investigations that permitted "gun walking." The OIG's review of ATF's Operations Wide Receiver and Fast and Furious revealed that ATF and the U.S. Attorney's Office for the District of Arizona did not manage these investigations responsibly and that hundreds of firearms that ATF agents could and should have interdicted ended up at multiple crime scenes in the United States and Mexico, including the scene of a U.S. Customs and Border Protection agent's murder.

The OIG determined that the investigations were plagued by several systemic problems, including inadequate attention to public safety, a lack of sufficient supervisory controls and oversight from ATF Headquarters, inappropriate use of cooperating federal firearms licensees as informants, and a failure to coordinate with other law enforcement agencies. In addition, the OIG found that the Department responded to a congressional inquiry about ATF firearms trafficking investigations with inaccurate information. Such incidents seriously tarnish the Department's reputation and greatly enhance the need to focus on restoring the public's confidence in the Department as an organization capable of protecting public safety.

The Department also faces challenges with respect to ensuring the fairness of its prosecutions, an issue that was the focus of recent Senate and House Judiciary Committee hearings on discovery concerns arising out of the failed prosecution of former Senator Ted Stevens. To achieve this goal, the Department must be able to conduct fair, objective, and accountable reviews of the conduct of its lawyers and other professionals, and to mete out appropriate discipline when it finds misconduct.

In our management challenges reports in prior years, the OIG has outlined concerns about the Department's disciplinary efforts. For example, the Department's Office of Professional Responsibility (OPR), by statute, has jurisdiction to investigate allegations of misconduct against Department attorneys acting in their capacity as lawyers. The OIG has long questioned this role for OPR because OPR is managed as a component of the Department, has no institutional independence, and lacks transparency insofar as it does not regularly release its reports and conclusions to the public. It is therefore unduly difficult – if not impossible – for the public to assess the consistency of OPR's findings and conclusions. The credibility of the Department's disciplinary decisions is inevitably reduced when the responsible components operate under the direction of the Department's senior leadership and without appropriate transparency.

Additionally, the OIG is examining the effectiveness of the discipline system used by U.S. Attorneys' Offices and the Executive Office for U.S. Attorneys when investigating allegations of employee misconduct. This review is the sixth OIG review since 2001 to assess a component's disciplinary system. Previous OIG evaluations examined the disciplinary systems of the USMS, BOP, DEA, ATF, and FBI and made many recommendations to these components, including a still-open recommendation from 2004 that the BOP develop procedures to ensure that discipline is imposed consistently throughout the agency. But the Department faces a broader challenge than simply ensuring that individual components maintain internally consistent and effective disciplinary system: it must also ensure that disciplinary procedures remain consistent across components so that all of the Department's employees, attorneys and non-attorneys alike, are held to the same tough but fair standards.

The Department also faces challenges with respect to ensuring the integrity of its hiring processes. In July 2012, the OIG issued a report finding that eight current or former JMD officials – many holding senior positions – violated applicable statutes and regulations in seeking the appointment of their relatives to positions within JMD. The OIG also found that a Deputy Assistant Attorney General in JMD responded inadequately to warning signs she received concerning the hiring of relatives of JMD employees. The 2012 OIG report marks the third OIG investigation in the last 8 years involving improper hiring practices within JMD, suggesting that prior management efforts to correct hiring practices in JMD have been inadequate. Adherence to fundamental federal hiring laws and regulations must be enforced to restore confidence in the fairness of the Department's hiring processes and the integrity of its operations.

The Department must also restore the public's confidence that the FBI Laboratory is using forensic techniques in accordance with strict protocols to ensure unbiased, objective, and reliable results. Between 1996 and 2004, a Department task force reviewed thousands of past prosecutions potentially affected by 13 FBI Laboratory employees whom the OIG criticized in an April 1997 report concerning the FBI Laboratory. The task force identified and referred many cases for independent scientific review. This review involved an examination of available lab reports, bench notes, and trial testimony; it did not include a re-examination of the original evidence. The task force then provided the results of these reviews to prosecutors who, in turn, were responsible for determining whether to disclose the material to the defendants pursuant to laws requiring the disclosure of exculpatory evidence. However, the task force never published a complete accounting

of the results of its review or the prosecutors' disclosures. At Congress's request, the OIG recently initiated a review of the task force's activities, processes, and decisions. Since the initiation of the OIG's current review of this matter, the FBI, in cooperation with the Department and the Innocence Project, announced that it will conduct a separate and new review of all case files involving FBI Laboratory hair and fiber examiners.

The Department's handling and use of informants also has affected the public's confidence in the Department. Among the most notable incidents was the FBI's failure to properly supervise Special Agent John Connolly, Jr.'s dealings with organized crime figures James "Whitey" Bulger and Stephen Flemmi. More recently, a former FBI agent, Adrian Busby, was convicted of making false statements when he lied to his supervisors and the OIG about his relationship with a female informant. The OIG's investigation determined that, after the informant came under investigation, Busby provided the informant and her defense attorney with copies of confidential FBI and Internal Revenue Service reports of interviews and also engaged in an inappropriate sexual relationship with the informant. Busby was sentenced to 1 year and 1 day for his crimes. Separately, the OIG found that ATF agents in both Operation Wide Receiver and Operation Fast and Furious used the substantial cooperation of federal firearms licensees to advance their investigations, creating at least the appearance that ATF agents approved or encouraged sales of firearms they knew were unlawful and did not intend to seize. In light of these missteps, the Department must focus its attention on ensuring the appropriate handling and use of informants.

The Department also must ensure the transparency of its operations. An important aspect of this effort is to avoid over-classifying its national security information, which can inhibit information sharing, increase the cost of information security, and unnecessarily limit the public's access to information. As required by the *Reducing Over-Classification Act*, the OIG is conducting a review to assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered, and to identify whether any of these rules and practices may contribute to misclassification of Department information.

The Department also has received criticism for its responses to requests for information pursuant to the *Freedom of Information Act* (FOIA). The Department has made progress in this regard, most notably by issuing a memorandum from the Attorney General in 2009 encouraging federal agencies to make discretionary disclosures of information and by launching www.FOIA.gov in 2011 to make data from agencies' annual FOIA reports more accessible and useful. Nevertheless, with roughly 60,000 FOIA requests handled in a decentralized fashion by 34 separate FOIA offices and the equivalent of 528 full-time FOIA employees, the Department faces a continuing challenge in ensuring that its own FOIA responses are consistent with each other and with the presumption of disclosure articulated the Attorney General's memorandum. In addition, as part of its review of the Voting Section of the Civil Rights Division, the OIG is investigating allegations that Department personnel gave preferential treatment to political allies in responding to FOIA requests.

Finally, the Department must encourage its employees to come forward and report information about waste, fraud, abuse, and mismanagement in the Department's operations and functions. Further, the Department must be committed to protecting the legal rights of those employees who do come forward. Whistleblowers play a crucial role in uncovering waste, fraud, abuse, and mismanagement, yet they are too often subject to retaliation for their disclosures. The OIG has conducted numerous investigations into allegations of retaliation, and we recently appointed an OIG Whistleblower Ombudsperson responsible for, among other things, ensuring that complaints of retaliation within the OIG's jurisdiction are reviewed and addressed in a prompt and thorough manner, and for communicating with whistleblowers about the status and resolution of such complaints. The OIG will continue to monitor this important issue.

7. Coordinating Among Law Enforcement Agencies: Law enforcement represents a central element of the Department's mission, yet the ability and willingness of Department components to coordinate and share intelligence, resources, and personnel with one another and other law enforcement agencies has historically posed a significant challenge.

One cause of this challenge is the confusion created when components have overlapping jurisdictions. The Department has four primary law enforcement agencies – the FBI, DEA, ATF, and USMS – yet these components' jurisdictions are not exclusive. For example, whereas the FBI may investigate all federal crimes and instances of terrorism, other agencies possess simultaneous jurisdiction to enforce specific criminal laws that necessarily overlap, such as the DEA's investigations of federal drug cases or ATF's investigations of federal firearms cases. The OIG highlighted this issue in its October 2009 report detailing coordination problems between ATF and the FBI in explosives investigations and made 15 recommendations to assist in improving coordination and reducing conflict between the FBI and ATF on explosives investigations and associated support activities. Five of these recommendations remain open, including our recommendation that the FBI and ATF develop certain protocols on joint investigations for explosives incidents. More recently, an April 2011 GAO report, entitled *Law Enforcement Coordination: DOJ Could Improve Its Process for Identifying Disagreements Among Agents*, described similar coordination problems that exist outside of the realm of explosives investigations.

Some overlap between these four components is unavoidable and may even help ensure proper law enforcement focus and attention. However, the Department should clarify the jurisdictional boundaries of each wherever possible. It may also benefit from considering whether consolidation of any operational functions or administrative functions, such as information technology, human resources, budgeting, and records management, could yield operational benefits, improve law enforcement safety, or save costs. Similarly, the Department should consider ways to increase the sharing of lessons learned and best practices among law enforcement components.

In the same vein, the Department should consider whether its law enforcement components have the proper level of consistency in their standard procedures, protocols, and manuals; where there are differences, the Department should consider whether they are justified. While the Department's law enforcement components generally adhere to Attorney's General Guidelines and policies for law enforcement activities, specific protocols and procedures for particular investigative techniques often vary from component to component. In particular, our review of new policies ATF implemented after Operation Fast and Furious underscored the agency's delay in completing its integration into the Department and in implementing controls to protect the public that were used in other Department law enforcement components. For example, we found that ATF had not until recently used review committees to evaluate either its undercover operations or its use of high-level and long-term confidential informants. We also expressed concern that ATF and the Department had not devoted sufficient attention to ensuring that ATF's policies scrupulously adhered to requirements found in the Attorney General's Guidelines and other Department policies, including ATF's confidential informant policies, which were not revised to conform to the Attorney General's Guidelines Regarding the Use of Confidential Informants until 8 years after ATF joined the Department. We therefore believe that Department-led, cross-component assessments designed to compare the law enforcement components' policies could identify opportunities for improvements that would make the Department's law enforcement operations more consistent and efficient.

Finally, opportunities may exist for the Department to better coordinate the collection and sharing of information used in law enforcement investigations. The OIG is reviewing one such effort already under way, the Organized Crime Drug Enforcement Task Forces (OCDETF) Fusion Center, an

intelligence and data center for drug and drug-related financial intelligence information from numerous member agencies and other sources, including the Treasury Department's Financial Crimes Enforcement Network (FinCEN). Our review is assessing the timeliness and value of the fusion center's analytical products and information sharing procedures.

8. Enforcing Against Fraud and Financial Offenses: The Department has long played an important role in preventing and reducing fraud and financial crimes, but rarely in the Department's history has this role received as much attention – or as many resources – as in the past few years.

From FY 2009 to FY 2011, with the country struggling to recover from the collapse of its housing market, the FBI received approximately $196 million from Congress to fund 156 new agents and 256 new non-agent positions devoted to combating mortgage fraud. During this same time period, the U.S. Attorneys received an additional $19.9 million in financial fraud funding, enough to fund 95 new attorney positions and 26 new non-attorney positions; the Criminal Division received $1.8 million in financial fraud funding for 5 new attorney positions and 2 new non-attorney positions; and the Civil Division received $10 million in financial rescue funding for 87 new attorney positions and 31 new non-attorney positions. The Department also requested an additional $55 million for FY 2013 to fund 328 new positions, including 40 FBI agents, 184 attorneys, 49 in-house investigators, 31 forensic accountants, and other administrative support, all to support the Department's efforts to investigate and prosecute financial fraud.

Resources alone, however, are not sufficient to address the problem of fraud and financial crime; the Department must also make the most of the tools and resources it has at its disposal. Prosecution and civil litigation are among the most important of those tools. For example, in September 2012, the Department announced that its total recoveries in *False Claims Act* cases since January 2009 exceeded $13 billion, of which $9.3 billion was recovered in cases involving fraud against federal health care programs. Many of those cases were the result of disclosures by whistleblowers, starkly demonstrating the importance of encouraging government employees to come forward with information about waste, fraud, abuse, and mismanagement. The Department should continue to strive to maximize such recoveries.

The Department has particularly targeted the problem of mortgage fraud. The Department reported in June 2012 a 92-percent increase in mortgage fraud prosecutions across the nation since FY 2009, and in February 2012, the Attorney General announced a $25 billion settlement with the nation's five largest mortgage servicers to address misconduct by the banks in bankruptcy cases involving inflated or inaccurate claims, improper accounting of mortgage payments, adding improper fees and charges to mortgage accounts, charging hidden fees to mortgage accounts, and other similar activities. The OIG is conducting an audit of the Department's strategy and approach to address mortgage fraud.

Another tool in the fight against fraud and financial crime is the Financial Fraud Enforcement Task Force (FFETF), an interagency working group established by the President in November 2009 and led by the Attorney General. With more than 20 federal agencies, 94 U.S. Attorneys' Offices, and state and local partners, the FFETF provides an unusual opportunity for a coordinated approach to the complex problem of fraud and financial crime. At the same time, an interagency effort of this scope also presents the significant challenge of coordinating these agencies' enforcement efforts, and the FFETF therefore requires strong leadership from the Department. Yet the FFETF is currently operating without an overall strategic plan that outlines its goals for preventing fraud and identifies how the effectiveness of the task force's efforts is to be measured. Nor has the FFETF published an annual report since 2010, its first year. We believe the FFETF has the opportunity to be more effective by uniting its members behind clear goals and by improving the accountability and transparency of its operations.

The Department has also prioritized the investigation of Residential Mortgage-Backed Securities (RMBS) fraud. The President, in his January 2012 State of the Union address, announced the creation of what became known as the Residential Mortgage-Backed Securities Working Group. The working group is intended to be a collaborative effort to investigate RMBS misconduct by looking for evidence of false or misleading statements, deception, or other misconduct by market participants in the creation, packaging, and sale of mortgage-backed securities. However, current budget uncertainties and the possibility of future budget constraints could cause future managerial challenges for the Department in fighting this area of financial fraud.

In addition, the Department must fight financial fraud both before and after it occurs. For example, the Department can use the suspension and debarment of individuals or entities to protect the government's financial interest from unethical, dishonest, or otherwise irresponsible entities and to reduce fraud, waste, and abuse in federal programs. Suspension and debarment decisions are made either administratively through agency suspending and debarring officials or statutorily as a result of convictions for qualifying offenses. In June 2012, the OIG completed an audit of the Department's implementation and oversight of statutory debarment activities from FY 2005 through FY 2010. Overall, the OIG found that the Department had not established an adequate system to ensure that it fulfills its responsibilities related to statutory debarment, creating the possibility that federal funding could be inadvertently and inappropriately awarded to excluded individuals. The OIG made 21 recommendations to the Department and its components to improve the effectiveness of statutory debarment programs, including recommending the development of additional policies and procedures to improve the completeness and accuracy of the reporting of debarment actions.

The Department also uses its Asset Forfeiture Program to confiscate both the means to commit and the proceeds of criminal activity. For FY 2011, the Department reported to Congress that it disposed of forfeited property valued at over $1.6 billion using methods such as liquidation and retention for official use. However, the Department may benefit from seeking greater interagency efficiency in its asset forfeiture efforts, as a recent GAO report concluded that there may be overlap between the asset management activities and the information technology infrastructures of the Department's Asset Forfeiture Program and the Treasury Department's similar Asset Forfeiture Fund. The Department may wish to consider studying the feasibility of consolidating or better coordinating the administrative structure of its asset forfeiture program with that of the Treasury Department.

9. Administering Grants and Contracts: The Department's management of grants and contracts has long presented a challenge by virtue of the large amounts of money at stake. From FY 2008 through FY 2011 the Department awarded approximately $15 billion in grants and $27 billion in contracts, and it awarded another approximately $1 billion in grants and $6 billion in contracts in FY 2012. Appropriate administration of public funds must always be a priority, but in this climate of constrained budgets, the use of billions of taxpayer dollars requires particular attention from Department management.

Grants

The OIG has previously noted the Department's demonstrated commitment to, and significant improvements in, the area of grant management. While we acknowledge the Department's continued efforts in this regard, we also believe that both challenges and opportunities for improvement remain.

The Department maintains three grantmaking components: the Office of Justice Programs (OJP), Office on Violence Against Women (OVW), and Community Oriented Policing Services (COPS).

This division of responsibility creates the challenge of ensuring that there is proper coordination of, and clear strategic vision for, its overall grantmaking efforts, and that those overall efforts are consistent with the priorities of the Department's non-grantmaking components. Prior OIG reports have found that improvements could be realized, particularly with regard to reducing duplication. For example, while OVW has in the past required its grant recipients to use the OJP financial guide, OVW has recently released its own financial guide. OVW grantees who also receive OJP grants therefore must often follow two different sets of rules, thereby increasing the risk of waste and noncompliance. A recent GAO report raised similar concerns, noting that COPS uses a different grant management system than OVW and OJP, thereby limiting the Department's ability to share information on the funding its components have awarded or are preparing to award. The Department should seek to consolidate the common functions of these three grantmaking components to increase coordination and save costs while maintaining key separate practices for meeting individual statutory requirements and fulfilling the missions of each office.

In addition to increased coordination, the Department should ensure that grants are achieving the intended results. The Department presented several outcome-oriented performance measures in its FY 2011 Performance and Accountability Report (PAR) that related to grants, yet many of those measures did not adequately measure the total return on investment a grant award has achieved. For example, the PAR included a measure of the percent reduction in DNA backlog, but it did not report the amount of resources used to achieve that reduction – a crucial element in any assessment of the success of DNA backlog-related grantmaking. Using performance measures that provide adequate information to evaluate not only the benefits achieved through the grantmaking process but also the investment required will help the Department improve the efficiency of its grantmaking and allow it to use its limited resources where they will be most useful.

Once grant funds are disbursed, the Department relies on thousands of governmental and non-governmental grant recipients to appropriately manage the billions of dollars of awards. It is imperative that the Department diligently oversee those recipients and provide them with tools to help ensure that grant terms and conditions are followed. Several such efforts are under way at the Department. For example, in September 2011, representatives from the Civil Division, the Antitrust Division, and the OIG, in cooperation with the Department's National Advocacy Center, produced a grant fraud training video for federal prosecutors and other government attorneys. In March 2012 the Financial Fraud Enforcement Task Force's Recovery Act, Procurement, and Grant Fraud Working Group, which includes the OIG, released a training framework for reducing grant fraud risk. The Department also developed and implemented a Grant Financial Management Online Training program complete with test questions to help support grant recipient compliance with rules and regulation. Yet not all of these training programs are required for all Department grant recipients, and as demonstrated by the $22 million in questioned costs reported in FY 2012 OIG grant and contract audits as well as related single audits, grant management and the oversight of grantee expenditures continue to be significant challenges for the Department.

Contracts

The Department spends more on contracts for goods and services each year than on grants. Some of the largest of these contracts are related to the planning, implementation, and management of complex information technology systems. For example, the Department awarded a contract of up to $512 million over 7 years to provide managed information technology services and secure technology solutions to ATF and the USMS. The Department's FY 2012 projections also included spending $220 million for the FBI's Next Generation Identification project to share fingerprint and other biometric information, $87 million for JMD's Law Enforcement Wireless Communications program, and $84 million for a Department-wide Unified Financial Management System, all under

Department-awarded contracts. In total, the Department awarded nearly $3 billion in contract funds on information technology in FY 2012.

The OIG's audits and reviews of Department programs have found instances of wasteful and poorly managed expenditures on information technology. For example, and as described above, the OIG's September 2012 audit of the FBI Laboratory's forensic DNA case backlog determined that two attempts and a combined $14 million since 2003 had failed to yield a system capable of electronically managing laboratory operations, and a new system is now in development. Additionally, the OIG's September 2012 interim report on the FBI's implementation of Sentinel, an investigative and case management system, found that the FBI deployed the system after taking over management of the project from a contractor. However, we found that the system was deployed behind schedule and did not provide all of the originally planned capabilities. We also found that although the FBI's $441 million cost estimate is $10 million less than the latest Sentinel budget, the estimate did not include originally planned operations and maintenance costs for the next 2 years, which the FBI estimated to be $30 million annually. Moreover, the FBI did not adjust its cost baseline when it transferred requirements to other FBI information systems. The Department must ensure that there is adequate management and oversight of information technology contracts to minimize cost overruns and provide planned system functionality.

Finally, the Department must ensure that it uses all the tools at its disposal to avoid awarding contracts to recipients who are likely to waste, embezzle, or mismanage the funds. For example, the Department should use suspension and debarment, described in detail above, to the fullest extent possible to protect the government's financial interest from unethical, dishonest, or otherwise irresponsible entities, and to reduce waste, fraud, and abuse in federal programs.

10. Ensuring Effective International Law Enforcement: According to the Administration's July 2011 *Strategy to Combat Transnational Organized Crime,* "[t]ransnational organized crime poses a significant and growing threat to national and international security, with dire implications for public safety, public health, democratic institutions, and economic stability across the globe." Moreover, transnational crime is no longer limited to organized crime. New communications technologies, the global banking system, and porous borders in international conflict zones have increasingly allowed criminals involved in terrorism, money laundering, gun trafficking, human trafficking, and myriad other crimes to operate internationally, thus creating new and daunting challenges for the Department's international law enforcement efforts.

In an effort to address this issue, the DEA, FBI, ATF, USMS, and the Department's Office of International Affairs (OIA) have stationed personnel abroad who work with their foreign counterparts to investigate and prosecute violations of U.S. law, and to provide reciprocal assistance to their foreign counterparts. The DEA maintains the Department's largest international presence with more than 1,000 full-time employees devoted to international operations in 65 countries. The DEA requested an international enforcement budget of more than $400 million in FY 2013. The FBI's international presence is also substantial, with 61 legal attachés, 14 sub-offices, and 287 authorized positions in 66 countries during FY 2012.

Devoting resources to transnational law enforcement efforts will not be enough: these resources must also be well managed, coordinated with each other, and coordinated with both domestic and foreign law enforcement organizations. Meeting these challenges requires putting frameworks in place to support international investigations before they begin, including clear lines of investigative authority among law enforcement agencies, appropriate mechanisms to share information, and appropriate and consistent training of all personnel involved in international operations. For example, the Department, and in particular the OIA, works to advance the government's interests in

extraditing defendants from abroad and in obtaining critical information through Mutual Legal Assistance Treaty (MLAT) requests and other means. Yet with many countries, the United States does not have effective legal mechanisms to permit the exchange of defendants or information. Ensuring that these mechanisms are in place – including bilateral and multilateral treaties, memoranda of understanding with foreign counterpart law enforcement agencies, and other agreements – will greatly enhance the Department's ability to fight crime at home and abroad.

International law enforcement operations also require robust supervision and oversight. The OIG's recently released report on ATF's Operation Fast and Furious vividly demonstrated the importance of this challenge – and the serious pitfalls and potential threats to public safety that await when law enforcement efforts fall short. Our report examined ATF's Operation Wide Receiver, an investigation conducted in 2006 and 2007, focusing on straw purchasers of firearms that were later transferred to Mexico. The primary goal of the operation was to allow straw purchases to continue in order to identify and prosecute members of the firearms trafficking organization. In service of that goal, ATF agents did not arrest the primary subjects involved in straw purchasing and seized less than a quarter of the more than 400 firearms purchased. ATF also worked with Mexican law enforcement to attempt failed surveillance operations of cross-border firearms shipments and developed a "cooperative agreement" with its Mexican counterparts. Yet ATF Headquarters neither vetted nor approved these joint efforts with Mexico, and we found no evidence that senior leaders in the Department had knowledge of Operation Wide Receiver until 2009. That a single ATF field office could have conducted this investigation without more oversight illustrates the shortcomings of ATF's case initiation and monitoring processes.

In addition to robust partnerships with foreign allies, effective and efficient international law enforcement requires cooperation and coordination with other federal agencies. For example, our examination of Operation Fast and Furious raised questions about how information was shared among various offices of ATF, the DEA, and the FBI. We also saw coordination and information sharing issues between ATF and U.S. Immigrations and Customs Enforcement (ICE), a component of the Department of Homeland Security. Our report noted instances where ATF resisted ICE conducting any independent or coordinated investigations that were related to Operation Fast and Furious through recovered firearms. In light of ICE's jurisdiction over export violations involving munitions and firearms, close coordination with ICE was essential in an investigation that purported to target a cartel in Mexico and had as a goal identifying the border crossing mechanism the cartel was using to obtain firearms from the United States.

The need for cooperation among federal agencies in the context of international law enforcement is not limited to investigative entities. In March 2012, the OIG released a report on the Office of Overseas Prosecutorial Development, Assistance and Training (OPDAT) and the International Criminal Investigative Training Assistance Program (ICITAP) offices in the Criminal Division that assist foreign prosecutors, law enforcement agencies, and governments to develop effective mechanisms to combat criminal conduct around the world. We found that while OPDAT's and ICITAP's relationships with most of their partner agencies were productive, their relationships with their primary funder, the State Department's Bureau of International Narcotics and Law Enforcement Affairs, warranted significant improvement during our review period. These strained relationships compromised OPDAT's and ICITAP's ability to make long-term international program plans and personnel retention decisions prior to 2012. Although the Department stated at the time of our report that these relationships had greatly improved, the inefficiencies we identified underscore the importance of working collaboratively with other federal agencies to address the growing challenge of international crime.

MANAGEMENT'S RESPONSE
TO THE OFFICE OF THE INSPECTOR GENERAL'S REPORT ON THE
TOP MANAGEMENT AND PERFORMANCE CHALLENGES
IN THE DEPARTMENT OF JUSTICE

FY 2012

The Department of Justice (the Department, DOJ) is the world's largest law office and the central agency for enforcement of federal laws. Its mission and responsibilities extend over the broad spectrum of American life. The Department appreciates the Office of the Inspector General's (OIG) recognition of its progress in addressing management and performance challenges facing this diverse institution. The Department's progress is an indication of agreement with the categories of top challenges in the OIG's report and represents the Department's commitment to prioritize and address these areas.

1 Safeguarding National Security

The Attorney General has said, "First and foremost: we will protect Americans from terrorism and other threats to national security – both at home and abroad." He has pledged to use every available and appropriate tool to obstruct terrorists at all stages of their actions around the world and in the United States.

To address the challenge of ensuring that national security information is appropriately shared among Department components and the Intelligence Community (IC), the Federal Bureau of Investigation's (FBI) Joint Terrorism Task Forces (JTTFs) coordinate with law enforcement across multiple jurisdictions. These Task Forces combine the resources of the FBI, the IC, state and local officers, and the military, and serve as a coordinating mechanism to investigate and share information regarding terrorism activity. In support of these efforts the FBI developed eGuardian to meet the challenges of collecting and sharing terrorism-related information. The eGuardian system serves as a single information repository for suspicious activity and is accessible to thousands of law enforcement personnel. Information captured in eGuardian is migrated to FBI internal systems and assigned to the appropriate JTTF for further investigation.

The Terrorist Watchlist maintained by the FBI's Terrorist Screening Center (TSC) is a database of identifying information about those known or reasonably suspected of being involved in terrorist activity. The Department is pleased that, to date, the OIG has closed 20 out of 23 recommendations stemming from its two watchlist reports. Currently, the OIG is assessing the accuracy, timeliness, and completeness of watchlisting practices, including nominations, modifications, and removals.

The FBI's Foreign Terrorist Tracking Task Force (FTTTF) partners with other government agencies to obtain data, conduct analyses, and provide investigative information to assist these agencies in detecting foreign national security threats. The FBI has implemented a strategy that provides significant value by performing in-depth analyses that proactively identify national security threats and assist ongoing national security investigations.

Another tool that the Department employs is national security letters (NSL). The Department is pleased that the OIG recognizes the FBI's progress in its use of NSLs while adhering to the legal requirements that protect civil liberties and privacy interests. The Department looks forward to the OIG's feedback to resolve the outstanding recommendations, many of which are part of the current USA Patriot Act Review.

2 Enhancing Cyber Security

The Department is keenly aware of the scope of cybersecurity threats and is collaborating with interagency partners and building relationships with private sector allies to address them. There is recent evidence that these threats are growing, and leaders of the IC have assessed that the threat of cyber-based terrorism, cyber-based espionage, and other state-sponsored cyber intrusions may eventually surpass that of terrorism generally. These threats present complex technical, legal, and jurisdictional challenges. They demand an all-tools response – including the use of the Department's law enforcement and intelligence capabilities.

The Department addresses cybersecurity threats in two capacities: first, as an agency responsible for detecting, disrupting, and deterring cyber threats, and second, as a government entity that is a potential target of cyber threats. DOJ has a primary role in domestic cyber incident response, and DOJ components are taking steps to improve their respective cybersecurity activities and to expand cross-component coordination of the Department's cybersecurity efforts. The principal components that investigate or conduct operational cybersecurity activities (the FBI, the Criminal Division (CRM), and the National Security Division (NSD)) each have active and ongoing outreach efforts to increase the private sector's awareness of these threats and to encourage the reporting of cyber incidents. The FBI, NSD, CRM, and the U.S. Attorneys' Offices (USAOs) also are increasing the use of prosecutorial tools against cyber threats to the national security.

In addition to bringing prosecutions against domestic criminal actors, the FBI, CRM, NSD, and over 200 Computer Hacking and Intellectual Property (CHIP) coordinators in USAOs around the country have continued to develop innovative means to disrupt, deter, and prosecute online criminal behavior, including through the use of civil tools and criminal forfeiture. For their part, the CHIP coordinators in each USAO have not only focused their efforts on prosecuting computer crime and intellectual property offenses, they also (1) serve as the district's legal counsel on matters relating to those offenses and the collection of electronic or digital evidence; (2) train prosecutors and law enforcement personnel in the region; and (3) conduct public and industry outreach and awareness activities. In addition, over the past year, departmental components have continued robust international outreach to ensure that DOJ's law enforcement partners abroad have the capacity to address computer crime within their countries, including by extraditing to the United States individuals involved in data breaches and other computer crimes.

Additionally, the Department has been at the forefront of addressing the information sharing and public-private sector cooperation necessary to secure and protect critical networks. The Department was integral in developing the Administration's proposed cybersecurity bill that would enhance information sharing in both directions between the federal government and the private sector, giving the private sector better information to direct its investments in security and enhance its defense against criminals and other threats to computer systems and information.

As noted in the OIG report, the Department's ability to achieve its strategic goals depends heavily on its ability to collect, process, manage, analyze, and share information. To meet mission investigative and information sharing requirements, DOJ's agents, attorneys, and analysts are increasingly reliant on connectivity to the Internet, to other DOJ components, and to multiple levels of government. This connectivity level increases the exposure of DOJ systems to disruption from cyber threats and attacks.

DOJ strives to stay abreast of cybersecurity issues and improve the protection of its critical systems and information from attack and compromise. The Department developed a comprehensive continuous monitoring program that enables all components and the Office of the Chief Information Officer (OCIO) to achieve near real time awareness on the security posture of its more than 230,000 information technology (IT) endpoint assets. In addition, the Department operates a 24/7 Security Operations Center

that monitors cyber threats and protects Department IT systems from cyber intrusions, attacks, espionage, and other cyber incidents. Regarding the remaining findings on contingency planning, identification and authentication, and audit and accountability controls, the Department developed rigorous plans of action and milestones for FY 2013 to help DOJ components correct these areas of weakness.

The Department has taken a leadership role to address the five classified information safeguarding priority areas identified by the Senior Information Sharing and Safeguarding Steering Committee. The Department OCIO worked closely with the FBI to consolidate DOJ classified circuits, with the results of significant security enhancements and cost savings. As noted in the report, the Department worked quickly to establish an Insider Threat Working Group comprised of components that access and process classified information. The Working Group has drafted Department policy, currently in final review, that establishes a Departmentwide insider threat detection and prevention program. This program, in addition to technology investments in the areas of enterprise audit, identity and access management, and removable media controls, will greatly reduce the risk of classified data loss within the Department.

DOJ's strategic security planning includes improvements in configuration management, identity and access management, security monitoring, auditing, alerting, and contingency planning. All of these enhancements leverage previous investments in security infrastructure and resources that form a strong foundation upon which the Department will continue to improve and respond to new and emerging cyber threats.

With regard to the *Federal Information Security Management Act* (FISMA) audits cited by the OIG, the Civil Division has fully implemented all seven of the OIG recommendations with respect to DOJ-owned equipment and equipment owned by most contractors, which comprise the vast majority of portable equipment potentially housing DOJ data. OIG has marked four of the seven recommendations "closed." The remaining three are outstanding only for equipment owned and operated by some outside experts, neutrals, and consultants hired under specific contracts. The solution for such contractors had been delayed due to technical issues with the Departmentwide encryption solution provided to the Civil Division. However, a pilot program for the outside contractor solution is nearing completion, and the Civil Division is preparing for full implementation.

While the recent FISMA audit identified control weaknesses in configuration management in the Bureau of Prison's (BOP) information security program, the audit concluded that the risk of compromising BOP's information security environment was low. Nevertheless, BOP took steps to monitor and track vulnerabilities and immediately implemented corrective action pertaining to configuration management such that the issue was resolved immediately and the risk that the deficiency would reoccur in the future was eliminated.

3 Managing the Federal Prison System

The Department appreciates the OIG's descriptions of the challenges the Federal Prison System faces. In addition to the alternatives to incarceration the OIG cited, the U.S. Parole Commission (the Commission) continues to work with its criminal justice partners to use alternatives to incarceration for low risk offenders that have demonstrated non-compliant behavior on supervision.

As an example, in 2012, the Commission began the Short-term Intervention for Success project, which is designed to assist low risk offenders in successfully completing their terms of supervision by use of short-term prison sanctions rather than longer prison terms. During the first year that the project has been in place, the average length of prison stay for prisoners that participated in the project has been 3.5 months compared to 11 months for prisoners committing similar violations of supervision during the 2-year period that preceded the pilot project. Since the pilot's inception, the overall number of prisoners held in

custody in the District of Columbia on a Commission warrant has been cut in half. The cost in jail bed days that is avoided by the reduced prison sentences has saved the federal government significant incarcerations costs. This is an evidence-based pilot program and the Commission will be evaluating whether recidivism rates are impacted by the shorter prison terms.

With respect to the OIG review of the Department's International Prisoner Treaty Transfer Program, the Department notes that only a small subset of the total number of foreign national prisoners incarcerated in the United States are either eligible to transfer to their native countries under the provisions of the applicable treaties or suitable to transfer after an analysis of the facts of each case. To clarify, the BOP's role in the treaty transfer process is limited with regard to determining eligibility and suitability. The BOP does not reject requests, but rather it reviews all inmate requests to determine if the inmate satisfies the requirements of the applicable treaty agreement and notifies the inmate of their apparent ineligibility. The BOP follows legally mandated guidance and applies the criteria to the requests. For example, the BOP uses criteria such as: the inmate has less than 6 months of the current sentence remaining to be served at the time of the request (France, Hong Kong, and Thailand require 12 months); the inmate has any pending proceedings, appeals, or collateral attacks – the judgment on the current conviction of sentence must be final. There are other equally concise criteria that the BOP applies to all requests. If an inmate believes the criteria were applied incorrectly, he can use the administrative remedy process to appeal. However, because the BOP applies a definitional process, not a judgmental one, to the requests, it is rare that an appeal is successful.

Just as challenging as the above are issues related to the sexual abuse of persons in the custody of the Department's BOP and the U.S. Marshals Service (USMS). As directed by the Prison Rape Elimination Act (PREA), the Department issued its final rule in May 2012 and is working to implement it throughout BOP and USMS facilities, including contract and Inter-Governmental Agreements facilities.

With regard to the prisoner work programs of Federal Prison Industries (FPI), the serious challenges to FPI's important reentry programs are not "business management practices" as mentioned by the OIG. Instead, fundamental changes to the economic and legislative environment in which FPI operates have diminished FPI's ability to market its products and provide for broader inmate employment and training opportunities. FPI is one of the BOP's most important reentry programs, one that reduces inmate recidivism by improving the job skills of inmates returning to society after serving their sentences. Unfortunately, FPI sales and revenues have significantly fallen in recent years, and, as the OIG indicates, more factories have been closed than opened since 2007. In addition to general economic and budgetary challenges affecting FPI, the change in its sales is also attributable to various legislative changes in Department of Defense authorization bills and various appropriations acts that have curtailed FPI's ability to enter into contracts with federal agencies. The Department's leadership, BOP leadership, and the FPI Board are acutely aware of the contracting and other budgetary dynamics affecting FPI's important programs, and will continue to seek opportunities to sustain FPI's programs. Among such approaches are an emphasis on finding repatriated off-shore work for FPI factories and a renewed emphasis on the use of job sharing for inmate workers.

4 Leading the Department in an Era of Budget Constraints

The Department has always faced budget constraints, but they have been greater over the past few years. As an agency whose mission requires that it often react to events, these constraints are felt across all DOJ components. Regardless, all components have developed strategies to work within these constraints, and the Department is pleased that the OIG recognizes these efforts.

In addition to typical approaches to address tight budgets, the Department proactively saves resources and uses them more efficiently. For example, the Attorney General's Advisory Council for Savings and

Efficiencies (SAVE Council) has saved $107.4 million to date by identifying opportunities for savings and implementing best practices Departmentwide. One example of component savings is the Drug Enforcement Administration's (DEA) approach to travel costs. In FY 2012, the DEA achieved savings of $6.5 million on travel costs by always choosing the lowest available airfares rather than customary government full refundable airfares.

Another SAVE Council initiative involves the Department advertising administrative forfeiture notices online. Because of the volume of administrative forfeiture notices, the Department expects to achieve an annual savings of $6.2 million. The Department currently offers the benefits of this online platform to other federal law enforcement agencies, including the U.S. Postal Inspection Service and the Secret Service. By expanding this program to more agencies, including Customs and Border Protection and Immigration and Customs Enforcement, even more taxpayers' dollars will be saved.

Both the DOJ and the Department of the Treasury (Treasury) have given serious on-going consideration to the Government Accountability Office (GAO) report recommending that the DOJ combine its Asset Forfeiture Program with that of the Treasury. While there are long-standing and significant differences between the operational and statutory environments of the two forfeiture programs, substantial benefits continue to be derived from adapting, whenever and wherever possible, the essential concept of economies of scale that is recommended by GAO. In this regard, judicial forfeiture cases are processed under one system for both forfeiture programs, and during FY 2012 a joint Claims Administration process was established to expedite the return of victims' assets forfeited under both programs. In FY 2013, a single joint international asset recovery support contract will be available to the investigative agencies of both programs.

Regarding long term planning for large IT systems, DOJ has maintained focus on the IWN program and, as noted in the OIG's report, changing circumstances have required the Department to change significantly the scope and deployment approaches for the IWN program over the last 10 years, thus adapting the program's spending during constrained and inconsistent funding periods. The IWN program's initial objectives were later reshaped due to advances in technology and the funding challenges of the program. Despite these challenges, as noted in the OIG Report, the Department has achieved significant improvements in the wireless communications capabilities delivered to DOJ's law enforcement agents.

The Department has maintained its commitment to implementing a secure, reliable, and interoperable Land Mobile Radio system for its tactical wireless communications. Additionally, the Department's Chief Information Officer (CIO), in conjunction with the Wireless Communication Board, provides oversight, governance, and management of resources associated with the IWN program to ensure efficiencies, reduce duplication, and improve economies of scale.

The Department is identifying and eliminating wasteful and duplicative IT spending. Several activities that were begun in FY 2012 to manage the Department's IT spending across the entire departmental portfolio will continue and expand in FY 2013. The Department is tracking all unclassified IT spending, allowing the Department to identify situations where duplicative component spending can be replaced with the use of shared resources. The Department also established commodity IT working groups in key areas such as email, data centers, telecommunications, and mobility. These cross-component groups are developing plans to consolidate IT assets and increase leveraged use of shared infrastructure. Another key area of work is strategic sourcing and vendor management. The Department will continue vendor management efforts begun in 2012 that include identifying strategic sourcing opportunities to pool the purchasing power of the Department.

Regarding the Department's debt collection efforts, in FY 2012, the Department collected $13.16 billion in criminal and civil actions - the highest amount ever and more than double the $6.5 billion collected in FY 2011. The $13.16 billion collected includes $3.03 billion in restitution, criminal fines, and felony assessments, and $10.12 billion in individually and jointly handled civil actions. In addition, $4.39 billion was collected through asset forfeiture actions in partnership with other divisions and agencies.

5 Protecting Civil Rights and Civil Liberties

The Department never loses sight of its responsibility to protect individuals' civil rights and liberties. This is more than just policy; protecting civil rights and civil liberties is part of the Department's culture and one of the Attorney General's identified priorities.

Discrimination persists in the education system, in the foreclosure crises, in America's workplaces, and in the voting booth. The Department uses a multifaceted program of enforcement designed to target and deter discriminatory conduct to: fulfill the promise of basic civil rights protections through effective and vigorous enforcement of the law; deter and remedy discriminatory and illegal conduct through the successful prosecution of these federal laws; and promote voluntary compliance and civil rights protection through a variety of education, technical assistance, and outreach programs.

The Department uses electronic surveillance techniques in some investigations because they are an effective law enforcement tool. At the same time, the Department recognizes that these court-authorized tools must be used carefully because if they are used inappropriately, they could intrude on civil liberties. The Department follows strict protocol when approving and using such techniques. In an effort to enhance its own approval process, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) updated and reissued guidance in April 2011 that reflects current laws and provides updated policies and procedures concerning approval and reporting requirements for the use of electronic surveillance. Another technology, unmanned aerial vehicles, also raises privacy and civil rights concerns. As a provider of grant funds to state and local governments to purchase equipment and technology that could be used for surveillance drones, the Department will ensure that grants used for funding drone technology will include requirements to ensure that federal funds are used in a manner consistent with applicable privacy and civil rights protections.

The Department is carefully monitoring court rulings and other legal proceedings related to the use of emerging technologies and modifying its investigative and prosecutorial guidance accordingly.

6 Restoring Confidence

The Department continues to strengthen its processes to maintain the public's trust in its fairness, integrity, and efficiency.

When the Attorney General learned of the ATF's flawed Fast and Furious operation, he ordered that the practices involved in that operation be stopped, he ordered the OIG to investigate the matter, and he instituted personnel changes and procedural reforms at the ATF. The ATF Acting Director issued a memorandum, dated November 3, 2011, clarifying policy concerning the transfer of firearms in the course of investigations. ATF established a monitored case program that ensures Headquarters' oversight of significant investigations. Additionally, ATF is completing a comprehensive revision to ATF's firearms transfer policy, which also addresses public safety, supervisory controls, and Headquarters' oversight of criminal investigations.

With respect to the OIG's concern that the Office of Professional Responsibility (OPR) has no institutional independence, the Department notes that OPR operates independently, with no interference from Department senior leadership. Actually, the OIG Report points to no instance in which Department senior leadership interfered with an OPR investigation, nor does it point to any OPR investigations that failed to hold Department leaders accountable. OPR has not hesitated to investigate senior Department leadership at the highest levels in the past, where appropriate, and to make misconduct findings against Department attorneys when the evidence supported such findings. Indeed, in FY 2012, OPR made professional misconduct findings in approximately 43% of the investigations it closed during the year.

To address the OIG's concern that OPR lacks transparency, OPR believes it is appropriately transparent, given the strict privacy protections afforded witnesses and subjects pursuant to the Privacy Act. In fact, the Privacy Act prevents OPR from releasing personal information about Department employees, except in limited circumstances.

With respect to the 2004 OIG Disciplinary Audit, the BOP continues to work to close the open recommendation. An unresolved issue regarding the Standards of Employee Conduct policy was litigated before the Federal Labor Relations Authority (FLRA). The FLRA ordered the agency to negotiate the union's proposal regarding its request for an employee to receive a copy of his affidavit during the course of Office of Internal Affairs and OIG investigations. The agency and the union have been unable to reach an agreement on this issue, but the BOP remains committed to resolving this matter and issuing the policy to meet the OIG's recommendation.

Regarding the OIG audit report on USMS Internal Affairs, a staffing shortage and a significant case backlog existed within Internal Affairs, the organization responsible for discipline within the USMS. However, as of August 2012, only 12 cases were older than 180 days. Additionally, the USMS has addressed its disciplinary system within its Strategic Plan. The USMS expects its latest update to the OIG regarding the status of open recommendations associated with this audit will close the audit report.

The Department's senior leadership took the OIG's findings in its report on the integrity of the hiring process within the Justice Management Division (JMD) very seriously. In response to the OIG report, the Assistant Attorney General for Administration (AAG/A) stressed to all JMD employees the importance of following the merit system principles, the prohibited personnel practices guidance, and the nepotism statute, all of which ensure a fair civil service system. In addition, the AAG/A instituted procedures to ensure that no inappropriate preferences in hiring occur in the future. Finally, the AAG/A appointed an impartial senior executive to review the employee and selecting official disclosures to ensure their confidentiality is preserved and that JMD is in compliance with all laws, policies, and regulations. As it did in the earlier cited instances, JMD will take appropriate action on the findings included in the OIG report.

The Department is focused on ensuring the transparency of its operations. It is committed to the full implementation of the "new era of open government" and the presumption of disclosure established in the President's and the Attorney General's Freedom of Information Act (FOIA) memoranda. Despite 3 straight years of receiving over 61,000 FOIA requests, the fourth highest number of requests received by any agency, the Department has made substantial efforts to ensure that requests consistently are processed in accordance with the FOIA and the President's and Attorney General's FOIA memoranda.

7 Coordinating Among Law Enforcement Agencies

The Department agrees with the OIG that its components must coordinate and share intelligence, resources, and personnel with one another and other law enforcement agencies. To address any possible confusion created within the Department due to overlapping jurisdiction among the four primary law

enforcement components (ATF, DEA, FBI, and USMS), the Department has worked to clarify roles and responsibilities when multiple organizations are involved in an incident or investigation.

Under the direction of the Deputy Attorney General, law enforcement components within the DOJ convened a De-confliction Working Group, consisting of representatives from DEA, FBI, USMS, ATF, and JMD, to examine the existing departmental de-confliction policies, procedures, and practices to further improve the efficient use of available resources and maximize the Department's performance. De-confliction of operational information such as persons of interest, investigative targets, and pre-planned enforcement operations is an essential element in all DOJ law enforcement investigations. Additionally, de-confliction facilitates the sharing of investigative information as well as the coordination among federal, state, and local law enforcement agencies.

To address the OIG's recommendation that the FBI and ATF develop a protocol for joint investigations of explosives incidents, the organizations have been working together, under the direction the Deputy Attorney General, on the jurisdictional overlap pertaining to explosives investigations. Since the *Deputy Attorney General's Explosives Protocol* was issued in FY 2010, the FBI and ATF have continued to resolve any lingering confusion over which entity should lead particular explosives investigations. They are developing plans and strategies to improve further the Department's coordination and management of explosives investigations. The Department has made significant progress toward resolving the jurisdictional concerns outlined in the OIG report. It has improved and integrated the databases for explosives-related information, improved law enforcement training for explosives investigations, and identified ways in which the FBI and ATF laboratories can work more efficiently and collaboratively on explosives investigations.

The OIG also recommends that the Department consider whether components' standards are appropriately consistent and notes that ATF's revision of several policies after Fast and Furious "underscores" ATF's delay in fully integrating with the Department and implementing controls already in place to protect the public. ATF has been working over the last year to ensure that all of its law enforcement policies are updated and consistent with Attorney General's Guidelines and policies for law enforcement activities. For example, in addition to establishing monitored case program management and updating its Firearm Enforcement Program policy, ATF has coordinated with other departmental components to update its confidential informant (CI) protocols. The results have produced a number of positive changes and additions to ATF's CI policy that will ensure effective approval processes for CIs and comprehensive de-confliction, not only within ATF but with other law enforcement agencies.

The OIG identified the Organized Crime Drug Enforcement Task Force's (OCDETF) Fusion Center (OFC) as one of the Department's efforts to share law enforcement information. The OFC is a key compartment in the Department's information sharing efforts. It supports numerous types of cases, including drugs, gangs, and transnational organized crime. In total the Department operates three fusion centers that support its law enforcement mission, the OFC, the Special Operations Division, and the El Paso Intelligence Center. These fusion centers, which address separate aspects of the enforcement process, combine the support of numerous federal partners, including participants from the Department, the IC, and other federal law enforcement agencies, as well as state, local, and foreign agencies. The law enforcement information sharing activities provided by these centers not only support case agents in the specific cases they are investigating, but they also link cases and agents through the information sharing process.

8 Enforcing Against Fraud and Financial Offenses

For the past several years, the Department has prioritized its efforts to eliminate fraud and other financial offenses and penalize those who commit them, and it has made use of the available tools, including prosecution, civil litigation, investigations, and task forces.

Some examples of the use of prosecution and civil litigation include the following: In the real estate sector, as a result of the Department's Antitrust Division's (ATR) efforts in FY 2012, 53 defendants pleaded guilty to real estate foreclosure and tax lien conspiracies across the United States that suppress and restrain competition in ways that harm communities and already financially distressed homeowners. In the municipal bonds industry, ATR's ongoing investigations have resulted in criminal charges against 20 former executives of various financial services companies and one corporation. Numerous financial institutions have agreed to pay a combined total of nearly $750 million in restitution, penalties, and disgorgement to federal and state agencies for their roles in the conduct.

As for the use of investigations, since the creation of the Health Care Fraud Prevention and Enforcement Action Team (known as "HEAT") in May 2009, preventing and shutting down health care fraud schemes have become top priorities for both DOJ and the Department of Health and Human Services (HHS). Joint DOJ/HHS Medicare Fraud Strike Forces are now operating in nine locations nationwide: Miami, Los Angeles, Detroit, Houston, Brooklyn, Baton Rouge, Tampa, Chicago, and Dallas. Since the first Strike Force was launched in 2007, these teams have charged more than 1,480 defendants for falsely billing the Medicare program more than $4.8 billion.

The Financial Fraud Enforcement Task Force (FFETF) is a tool that was established by the President in 2009 and is led by the Attorney General. The FFETF's mission, enumerated in the Executive Order creating it, is to (i) enhance coordination and cooperation among government agencies responsible for the investigation and prosecution of significant financial crimes and violations, (ii) strengthen the efforts of the Department of Justice and other federal, state, and local agencies to investigate and prosecute significant financial crimes and other violations relating to the financial crisis and the recovery efforts, (iii) protect the public and encourage greater coordination in the detection and prosecution of financial crimes through extensive outreach and educational opportunities, and (iv) support victims of financial crimes. While the Task Force's goals are ambitious, its foundation is rooted in simplicity: those charged with protecting the public in all levels of government cannot work in isolated and compartmentalized silos. Instead, the government is unified in its approach and execution, and it can achieve more by having its many offices and agencies working together than it ever could with the organizations acting separately.

In FY 2012 the FFETF created two additional working groups, the Residential Mortgage-Backed Securities (RMBS) Working Group and the Consumer Protection Working Group, both of which already have produced identifiable results. For example, the RMBS Working Group is overseeing active investigations by various DOJ components, numerous USAOs, and other government and state agencies and offices. Recently it announced the filing of a civil complaint against J.P. Morgan Securities LLC (formerly known as Bear Stearns & Co. Inc.), JP Morgan Chase Bank N.A., and EMC Mortgage LLC (formerly known as EMC Mortgage Corporation) by the Office of the New York Attorney General (a Working Group co-chair) based in part on the substantial assistance provided by the Department and other Working Group members. The suit was filed against these defendants for making fraudulent misrepresentations and omissions to promote the sale of residential mortgage-backed securities to investors. These defendants allegedly deceived investors concerning the way with which they evaluated the quality of mortgage loans packaged into residential mortgage-backed securities prior to Bear Stearns & Co's collapse in early 2008, incurring losses that have totaled approximately $22.5 billion to-date.

The Department agrees with the OIG that transparency and accountability of the FFETF are important. That is a principle reason the FFETF initially established a public website, www.stopfraud.gov, which frequently contains updates of the efforts of the various Task Force members and their activities, as well as provides educational resources for the public. Significantly, in an effort to reach an even larger population, the Victims' Rights Committee, which maintains the website, recently added a web-page containing Spanish-language resources for victims of financial fraud crimes. The FFETF will continue to examine new ways it can expand its reach, as well as continue to publish the results of its work, to the extent practicable.

Last, although the resources of the FFETF RMBS Working Group are frequently a topic of public discussion, the group has been performing quite well with its existing resources. Currently, it has more than 200 attorneys, investigators, analysts, and staff actively engaged in these investigations, and another dozen USAOs that have assisted with witness interviews around the country. The President's budget request for FY 2013 includes $55 million to assist the Department in fighting financial fraud, including RMBS fraud, in such ways as funding more FBI agents, prosecutors, civil attorneys, in-house investigators, and forensic accountants.

The Department agrees that suspension and debarment are powerful administrative tools which, when used appropriately, help protect the government's financial interests from unethical, dishonest, or otherwise irresponsible entities, as well as help reduce waste, fraud, and abuse. The Department's Suspending and Debarring Official (SDO) has actively used these tools in cooperation with the OIG to the fullest extent possible. For example, in calendar year 2011, the OIG referred 27 cases to the SDO recommending suspension or debarment, and the SDO issued notices of suspension or proposed debarment in 22 cases. The SDO also issued a notice to show cause in one case, entered into an administrative agreement in one case, and declined to initiate proceedings in one case involving an organization and three employees. Thus far in calendar year 2012, the OIG has referred 28 cases to the SDO, and the SDO has issued notices of suspension or debarment in 26 cases and proposed the debarment of the organization rather than two of its employees in the final two cases.

Meanwhile, to increase the integrity of the participants in the investigation and prosecution processes related to fraud and other financial offenses, on January 30, 2012, the Attorney General issued a policy statement on parallel proceedings that updated and strengthened the Department's longstanding policy that its "prosecutors and civil attorneys coordinate together and with agency attorneys in a manner that adequately takes into account the government's criminal, civil, regulatory and administrative remedies." Pursuant to this policy statement, and in an effort to ensure that suspension and debarment officials at government agencies have greater access to publicly-available information on corporate defendants that would permit them to pursue debarment and suspension remedies as appropriate, the Deputy Attorney General directed that all litigating components provide corporate criminal case information to the Interagency Suspension and Debarment Committee quarterly.

Regarding the Department's Asset Forfeiture Program, as was stated in the Department's response to Challenge #4, the Department concurred with the GAO's recommendation and is working with the Treasury forfeiture program to conduct a joint study to assess the feasibility of consolidation in the areas of asset management and asset tracking systems. The study will take into account the costs, benefits, and key questions to consider when determining whether consolidation could realize increased efficiencies, effectiveness, and cost savings.

9 Administering Grants and Contracts

Grants

The Department's grant making components, the OJP, the Office on Violence Against Women (OVW), and the Community Oriented Policing Service (COPS), have significantly improved collaboration and information sharing among themselves and other federal agencies to reduce duplication, identify cost efficiencies, and address common issues. The DOJ Grants Management Challenges Workgroup, established by the Associate Attorney General's Office and comprised of grants officials from COPS, OJP, and OVW, meets to develop consistent practices and procedures in a wide variety of grant administration and management areas. For example, in January 2012, the Department issued policy and procedures developed by the Grants Management Challenges Workgroup to implement the DOJ-wide high risk grantee designation program.

In recent months, COPS, OJP, and OVW have taken a number of actions in response to the recent GAO recommendations pertaining to potential duplication and overlap. DOJ currently is conducting a study to identify opportunities for shared grants management services. The first phase of the study, completed in August 2012, focused on documenting each component's award life cycle and identifying the areas of commonality across functional requirements to better assess the feasibility of a shared solution from a systems perspective. The study found a high degree of commonality and the potential for greater collaboration among the grant making components. Based on these findings, the Department will conduct an assessment to better understand the extent to which the Department's grant programs overlap with one another and determine if grant programs may be consolidated to mitigate the risk of unnecessary duplication. Using the results from the assessment, DOJ will be in a better position to develop a targeted and strategic approach to carry out a review of applications across all three components during the pre-award process. As part of this approach, DOJ will work to establish policies and procedures to govern this coordinated effort.

Meanwhile, COPS, OJP, and OVW have been engaged in an IT shared services feasibility analysis. During the first phase of the project, and after reviewing the current systems and business requirements, the contractor concluded that sharing a grants system was feasible, but that without enhancements, neither OJP's system nor COPS' system could support the business needs of each component. The two offices currently are beginning phase two of the project which will assist them with identifying the most feasible option for sharing IT services. This may include enhancing an existing system, building a new system, or sharing data through a data warehouse.

Regarding performance measurement, the Department is constantly trying to develop more meaningful measures for its grant making components. OJP is improving the quality and usefulness of the performance data collected from state, local, and tribal partners to help the agency make better informed programmatic and funding decisions. OJP recently initiated a new Performance Management effort aimed at integrating high-quality, reliable data into performance reporting and its operations, specifically grant monitoring, strategic planning, and management decision-making. As a first step in this effort, in FY 2013, OJP will carry out a thorough assessment of its current business processes related to performance measurement.

The COPS' performance goal is to obtain COPS-related contribution to a 3% rate of change over 36 months in homicide violent crime rates. COPS will implement a comprehensive community policing strategy within targeted COPS-funded cities and compare the crime rates of those cities with cities of similar size and demographics that have not received COPS funding. Also, beginning in FY 2013, COPS will implement the Homicide Reduction Measure to determine if grant funding is achieving the intended results.

The Department is dedicated to improving continuously its oversight and monitoring of grantees and grant programs. OJP consistently exceeds its statutory requirement to conduct comprehensive monitoring of not less than 10% of total award dollars. In FY 2012, OJP monitored more than twice the award amount required by law. It also conducts annual desk reviews on each of its nearly 14,000 grants. COPS also has a comprehensive monitoring strategy that entails programmatic and financial oversight of all of its grantees. The COPS Monitoring Division conducts both on-site and office-based grant reviews. Each visit, whether on-site or in the office, is supported with an exhaustive monitoring report that captures an extended list of requests, potential problems, documented issues, and recommendations. During FY 2012, the Monitoring Division managed 144 on-site grantee monitoring visits totaling 222 grants valued at over $276 million.

The grant-making components also closely coordinate with grantees and the OIG to address issues identified in grant audits and resolve outstanding audit recommendations in a timely manner. They have worked proactively and collaborative with the OIG on significant new programs that pose special risks, such as the Presidential Nominating Convention Security Funding, to ensure that all steps are taken to mitigate the risks with such large and/or complex funding programs.

To help grant recipients follow grant terms and conditions, the Department ensures grantees have access to tools and training necessary to effectively implement and manage their programs. The Grant Management Challenges Workgroup created an on-line grantee financial management training program. In December 2011, the Department launched this comprehensive on-line training tool for all DOJ grantees and grant management staff. The OIG described this training as a tool to help ensure that grant terms and conditions are followed, and to support grant recipients' compliance with rules and regulations. On-line training has increased the accessibility of DOJ's grant recipients to financial management administration and program compliance requirements and has been highly rated by those using the tool. In addition, under the DOJ High Risk Policy, grantees designated as high-risk receive an automatic special condition on all new DOJ awards that requires them to take financial management training.

Contracts

The Department spends large amounts on contracts each year, and it closely monitors the cost, timeliness, and quality of requested goods and services. As noted by the OIG, some of the largest of these contracts are related to planning, implementation, and management of complex information technology systems. The Department, under the direction of its new Chief Information Officer, is examining its entire IT portfolio and is exploring opportunities for leveraged buying and strategic sourcing of IT commodities and services.

With regard to the OIG's comments on the FBI's Sentinel system, the FBI successfully deployed Sentinel in July 2012. The Department notes that the FBI did not eliminate or reduce any of the Sentinel requirements to stay within the $451 million budget allocation. However, IT has changed significantly since system requirement specifications were developed 7 years ago. Since October 2010, Sentinel executives and stakeholders have completed several comprehensive reviews of the requirements necessary to achieve the objectives set out for Sentinel. Some requirements changed to take advantage of new technology. Additional functionalities originally planned for Sentinel continue to be provided more

effectively by other systems that remain online irrespective of Sentinel. The Department notes that implying that Sentinel was in any way deficient for "not providing all of the originally planned capabilities" is misleading. Because of the dynamic nature of the FBI's development process, the FBI deployed Sentinel for approximately $10 million less than had been budgeted. Beyond reporting the actual cost of the project, $441, there is no "cost baseline" to adjust.

The Department agrees that it "must ensure that there is adequate management and oversight of information technology contracts to minimize cost overruns." This aspect of the recommendation, however, is out of place following a discussion of Sentinel. The Sentinel project did not suffer from cost overruns; it came in under budget. As for the other aspect of the recommendation, rather than ensuring that an IT project "provide[s] planned system functionality" statically, as initially conceived even if that was years before deployment, Sentinel serves as a model of dynamic reassessment and refinement of a project's required functionality. Sentinel has not failed to provide any appropriate functionality; data provided to the OIG confirms that the FBI has recognized significant efficiency gains in just the first few months since deployment.

10 Ensuring Effective International Law Enforcement

As the OIG states, in an effort to address the threat of transnational organized crime, the DEA, FBI, ATF, USMS, and the Criminal Division's Office of International Affairs (OIA) have stationed personnel abroad to work with their foreign counterparts to investigate and prosecute violations of U.S. law. To build and nurture relationships with law enforcement counterparts, the Department works with host nation counterparts through vetted units, legal attaches, and other personnel stationed overseas. A large amount of the Department's international work, however, takes place in its domestic offices. For example, in addition to its 10 prosecutors stationed abroad, OIA has an additional 50 attorneys and 35 paralegals in Washington, DC. Similarly, the Department's law enforcement components have substantial numbers of personnel within the United States who are pursuing international cases and who work in collaboration with personnel posted overseas.

The Department agrees with the OIG that devoting resources to transnational law enforcement efforts will not be enough, that the resources must also be well managed, coordinated with each other, and coordinated with both domestic and foreign law enforcement organizations.

The Department recognizes that there always will be issues and differences that must be worked out with other organizations, regardless of whether those organizations are foreign or domestic. The OIG references the Criminal Division's Office of Overseas Prosecutorial Development, Assistance and Training (OPDAT) and its International Criminal Investigative Training Assistance Program (ICITAP) offices and their relationship with their primary funder, the State Department (State). While both OPDAT and ICITAP have responsibilities that are strictly focused on assisting foreign entities – training prosecutors, law enforcement agencies, and governments, they work very closely and collaboratively with their international counterparts. However, the complexity of funding for international activities presents challenges that the Department continues to address.

This page intentionally left blank

FMFIA

Corrective Action Plan

FMFIA SECTION 2 – PROGRAMMATIC MATERIAL WEAKNESS – PRISON CROWDING

U.S. DEPARTMENT OF JUSTICE **Corrective Action Plan** **Issue and Milestone Schedule**	**Report Date** September 30, 2012	
Issue Title	**Issue ID**	**Component Name**
Prison Crowding	06BOP001	Bureau of Prisons

Issue Category

FMFIA, Section 2	☐	**Reportable Condition**	☒	**Material Weakness**
FMFIA, Section 4	☐	**Non-conformance**		
OMB A-123, Appendix A	☐	**Reportable Condition**	☐	**Material Weakness**

Issue Category – SAT Concurrence or Recategorization

Concur

Issue Description

As of September 30, 2012, the inmate population housed in BOP operated institutions exceeded the rated housing capacity by 38 percent. The BOP's Long Range Capacity Plan relies on multiple approaches to house the increasing federal inmate population, such as contracting with the private sector and state and local facilities for certain groups of low-security inmates; expanding existing institutions where infrastructure permits, programmatically appropriate, and cost effective to do so; and acquiring, constructing, and activating new facilities as funding permits.

To address this material weakness, the BOP will continue implementing its Long Range Capacity Plan, making enhancements and modifications to the plan, as needed, commensurate with funding received through enacted budgets. The BOP's formal Corrective Action Plan includes utilizing contract facilities; expanding existing institutions; and acquiring, constructing, and activating new institutions as funding permits. The BOP will continue to validate progress on construction projects at new and existing facilities through on-site inspections or by reviewing monthly construction progress reports.

This material weakness was first reported in 2006. Remediation of the weakness through increasing prison capacity is primarily dependent on funding. Other correctional reforms and alternatives will require policy and/or statutory changes. Other initiatives notwithstanding, if the acquisition, expansion, construction, and activation plans detailed in the BOP's Long Range Capacity Plan are funded as proposed, the over-crowding rate for FY 2018 is projected to be 44 percent.

The Department's corrective action efforts are not limited to the BOP alone. The Department continues to consider and implement an array of crime prevention, sentencing, and corrections management improvements that focus on accountability and rehabilitation, while protecting public safety. The Department recognizes that the BOP's capacity management efforts must be teamed with targeted programs that are proven to reduce recidivism and promote effective re-entry. The BOP will continue to work with the Department on these programs.

Business Process Area (N/A for Section 2 and Section 4 issues)			
Not Applicable			
Date First Identified	**Original Target Completion Date**	**Current Target Completion Date**	**Actual Completion Date**
2006	09/30/2012	Dependent on funding	
Issue Identified By	**Source Document Title**		
Bureau of Prisons	BOP Population Projections		

Description of Remediation

Increase the number of federal inmate beds to keep pace with projected increases in the inmate population. Efforts to reach this goal include expanding existing institutions, acquiring surplus properties for conversion to correctional facilities, constructing new institutions, utilizing contract facilities, and exploring alternative options of confinement for appropriate cases.

Milestones	Original Target Date	Current Target Date	Actual Completion Date
1. As of September 30, 2006, the inmate population in BOP owned and operated institutions reached 162,514 and was housed in a capacity of 119,510, resulting in an over-crowding rate of 36 percent.	09/30/2006		09/30/2006
2. As of September 30, 2007, the inmate population in BOP owned and operated institutions reached 167,323 and was housed in a capacity of 122,189, resulting in an over-crowding rate of 37 percent, an increase of 1 percent for the year.	09/30/2007		09/30/2007
3. As of September 30, 2008, the inmate population in BOP owned and operated institutions reached 165,964 and was housed in a capacity of 122,366, resulting in an over-crowding rate of 36 percent, a decrease of 1 percent for the year.	09/30/2008		09/30/2008
4. As of September 30, 2009, the inmate population in BOP owned and operated institutions reached 172,423 and was housed in a capacity of 125,778, resulting in an over-crowding rate of 37 percent, an increase of 1 percent for the year.	09/30/2009		09/30/2009
5. As of September 30, 2010, the inmate population in BOP owned and operated institutions reached 173,289 and was housed in a capacity of 126,713, resulting in an over-crowding rate of 37 percent, the same rate as at the end of the previous year.	09/30/2010		09/30/2010
6. As of September 30, 2011, the inmate population in BOP owned and operated institutions reached 177,934 and was housed in a capacity of 127,795, resulting in an over-crowding rate of 39 percent, an increase of 2 percent for the year.	09/30/2011		09/30/2011
7. As of September 30, 2012, the inmate population in BOP owned and operated institutions reached 177,556 and was housed in a capacity of 128,359, resulting in an over-crowding rate of 38 percent, a decrease of 1 percent for the year.	09/30/2012		09/30/2012
8. Planning estimates call for a rated capacity of 130,404 to be reached by the end of FY 2013. The over-crowding rate is projected to be 40 percent at that time, an increase of 2 percent for the year.	09/30/2013		
9. Planning estimates call for a rated capacity of 134,170 to be reached by the end of FY 2014. The over-crowding rate is projected to be 39 percent at that time, a decrease of 1 percent for the year.	09/30/2014		
10. Planning estimates call for a rated capacity of 135,130 to be reached by the end of FY 2015. The over-crowding rate is projected to be 39 percent at that time, the same rate as projected for the end of the previous year.	09/30/2015		

11. Planning estimates call for a rated capacity of 136,430 to be reached by the end of FY 2016. The over-crowding rate is projected to be 40 percent at that time, an increase of 1 percent for the year.	09/30/2016		
12. Planning estimates call for a rated capacity of 136,430 to be reached by the end of FY 2017. The over-crowding rate is projected to be 42 percent at that time, an increase of 2 percent for the year.	09/30/2017		
13. Planning estimates call for a rated capacity of 136,942 to be reached by the end of FY 2018. The over-crowding rate is projected to be 44 percent at that time, an increase of 2 percent for the year.	09/30/2018		

Reason for Not Meeting Original Target Completion Date

Funding received through enacted budgets for additional capacity has not kept pace with the increases in the federal inmate population.

Status of Funding Available to Achieve Corrective Action

FY 2013 funding is unknown at this point because the FY 2013 budget has not been enacted. The Department of Justice's proposed FY 2014 budget for BOP is under review at the Office of Management and Budget.

Planned Measures to Prevent Recurrence

The BOP will continue to structure budget requests to address capacity needs in the most cost effective manner possible.

Validation Indicator

Results are measured as a new institution or expansion project is activated and resulting increases in rated capacity are established. A corresponding decrease in the over-crowding rate will also be a tangible measurement of the results. Progress on construction projects at new and existing facilities will be validated via on-site inspections of each facility or by review of monthly construction progress reports.

Organizations Responsible for Corrective Action

BOP Administration Division and Program Review Division

This page intentionally left blank.

Undisbursed Balances in Expired Grant Accounts

Section 536 of the Commerce, Justice, Science, and Related Agencies Appropriations Act, 2012 (Act) of the Consolidated Appropriations Act, 2010 (Pub. Law 112-55) requires certain departments, agencies, and instrumentalities of the United States Government receiving appropriations under the Act to track undisbursed balances in expired grant accounts for FY 2012.

Undisbursed balances in expired grant accounts include budget authority that is no longer available for new obligations but is still available for disbursement. According to Section 20.4(c) of OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget,* the expired phase "lasts five years after the last unexpired year unless the expiration period has been lengthened by legislation. Specifically, you may not incur new obligations against expired budget authority, but you may liquidate existing obligations by making disbursements." For FY 2012, the below information is required to be reported in the Performance and Accountability Reports and annual performance plans/budgets with regard to undisbursed balances in expired grant accounts: 1) details on future action the department, agency, or instrumentality will take to resolve undisbursed balances in expired grant accounts; 2) the method that the department, agency, or instrumentality uses to track undisbursed balances in expired grant accounts; 3) identification of undisbursed balances in expired grant accounts that may be returned to the Treasury of the United States; 4) in the preceding three fiscal years, details on the total number of expired grant accounts with undisbursed balances (on the first day of each fiscal year) for the department, agency, or instrumentality and the total finances that have not been obligated to a specific project remaining in the accounts.

Three Department of Justice grant-making agencies are required to report under this guidance: Community Oriented Policing Services (COPS), Office of Justice Programs (OJP), and the Office on Violence Against Women (OVW). Their responses are noted below:

Details on future actions that will be taken to resolve undisbursed balances in expired grant accounts:

COPS closely monitors the financial activity of all grantees. This includes requiring all grant recipients to report the financial expenditures for all COPS awards on a quarterly basis. COPS also maintains a group of dedicated Grant Program Specialists and Staff Accountants that offer grantees real-time technical assistance with implementing any aspect of their grant. Due to the additional reporting requirements and transparency associated with American Recovery and Reinvestment Act of 2009 (ARRA) grant recipients, COPS has implemented additional efforts to monitor COPS Hiring Recovery Program (CHRP) grantees. First, all CHRP grantees are required to complete an online grants management training, which includes a training track specifically addressing financial reporting and disbursement of funds. Second, CHRP grantees were notified earlier this year that the undisbursed balance on their grant awards will lapse on September 30, 2015 (5 years after the last unexpired year for ARRA), thus all grant program requirements should be completed by that time and all expensed funds disbursed. Third, beginning in November 2010, COPS conducts quarterly outreach efforts to a select group of CHRP grantees who appear to have either discrepancies in the financial or programmatic reporting on their awards. Finally, the COPS Director receives monthly and quarterly reports of CHRP activity, including disbursement data, and COPS management works with the Justice Management Division (JMD), OMB, and the Office of the Vice President (OVP) to ensure that ARRA funds are being disbursed and outlayed timely.

All OJP discretionary/categorical and block/formula grantees are required to submit a financial report quarterly. Grantees have 90 days after the end date of the award to drawdown funds and close out the award. If the payments to the grantee are less than the amount of the grant expenditures, then the grantee is given the opportunity to draw down these funds. OJP Customer Service Outreach staff calls the grantee

to ask them to draw down their funds. The first notice will commence on the same day as the phone call to the grantee. If the grantee has not drawn down their available funds after 14 calendar days, a second contact is made by the Customer Service Outreach staff and a second notice is sent. If there is no action by the grantee, a third notice is sent to the grantee informing them that OJP will de-obligate the funds from their grant. If the grantee has not retrieved their funds after 14 additional calendar days, the funds are de-obligated. After deobligation, the grantee will receive a Grant Adjustment Notice (GAN) in the mail informing them that the funds have been de-obligated and are no longer available and the grant is closed.

OVW closely monitors the financial activity of all grantees. All grant recipients are required to report their financial expenditures for OVW awards on a quarterly basis and their project performance activities on a semi-annual or annual basis. ARRA grantees are also required to submit special Section 1512 reports on a quarterly basis that include project and financial information. OVW reviews 100 percent of these reports for each reporting period and contacts the grantees regarding any concerns or questions. OVW has Grant Program Specialists and Financial Analysts that offer ARRA grantees technical assistance with implementing any aspect of their grant, including trainings, outreach, site visits and monitoring. The OVW management receives and reviews frequent reports on ARRA grant activity, including obligation and outlay data, and OVW management works with JMD, OMB, OVP, and the OIG to ensure that ARRA funds are being disbursed and outlayed timely.

Method used to track undisbursed balances in expired grant accounts:

COPS utilizes both the Financial Management Information System 2 (FMIS2) data as well as data from OJP's Grant Payment Request System (GPRS) to track CHRP undisbursed balances. OJP currently uses its Grants Management System (financial reports), FMIS2 and GPRS to track undisbursed balances. OVW utilizes both FMIS2 data as well as data from OJP's GPRS to track undisbursed balances.

Identification of undisbursed balances in expired grant accounts that may be returned to the Treasury:

The Department has the authority to transfer unobligated balances of expired appropriations to the Working Capital Fund. Specifically, Public Law 102-140 provides that at no later than the end the fifth fiscal year after the fiscal year for which funds are appropriated or otherwise made available, unobligated balances of appropriations available to the Department of Justice during such fiscal year may be transferred into the capital account of the Working Capital Fund to be available for the Department-wide acquisition of capital equipment, development and implementation of law enforcement or litigation related automated data processing systems, and for the improvement and implementation of the Department's financial management and payroll/personnel systems. Therefore, in general unobligated and undisbursed balances in the Department’s expired grant accounts will be transferred to the Working Capital Fund for use as authorized by law, not returned to the Treasury. An exception to this will be American Recovery and Reinvestment Act grant funds; pursuant to Public Law 111-203, such grant funds that have not been obligated as of December 31, 2012, will be rescinded and returned to the Treasury.

The total number of expired grant accounts with undisbursed balances (on the first day of each fiscal year) and the total finances that have not been obligated to a specific project remaining in the accounts, are as follows (dollars in millions):

OJP:
FY 2008: 9 accounts; $105.5 in undisbursed and unobligated balances
FY 2009: 10 accounts; $66.0 in undisbursed and unobligated balances
FY 2010: 8 accounts; $1,638.6 in undisbursed and unobligated balances
FY 2011: 6 accounts; $859.7 in undisbursed and unobligated balances
FY 2012: 5 accounts; $485.6 in undisbursed and unobligated balances

COPS:
FY 2008: No undisbursed and unobligated balances
FY 2009: No undisbursed and unobligated balances
FY 2010: 1 account; $1,001.9 in undisbursed and unobligated balances
FY 2011: 1 account; $861.8 in undisbursed and unobligated balances
FY 2012: 1 account; $580.3 in undisbursed and unobligated balances

OVW:
FY 2008: No undisbursed and unobligated balances
FY 2009: No undisbursed and unobligated balances
FY 2010: 1 account; $223.0 in undisbursed and unobligated balances
FY 2011: 1 account; $154.4 in undisbursed and unobligated balances
FY 2012: 1 account; $63.2 in undisbursed and unobligated balances

This page intentionally left blank.