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.