Top Management and Performance Challenges Facing the Department of Justice - 2013

December 11, 2013
Re-issued December 20, 2013

MEMORANDUM FOR: THE ATTORNEY GENERAL
THE DEPUTY ATTORNEY GENERAL

FROM: MICHAEL E. HOROWITZ
INSPECTOR GENERAL

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

Attached to this memorandum is the Office of the Inspector General's (OIG) 2013 list of top management and performance challenges facing the Department of Justice (Department), which we have identified based on our oversight work, research, and judgment. We have prepared similar lists since 1998. By statute this list is required to be included in the Department's Agency Financial Report.

This year's list identifies six challenges that we believe represent the most pressing concerns for the Department. They are *Addressing the Growing Crisis in the Federal Prison System*; *Safeguarding National Security Consistent with Civil Rights and Liberties*; *Protecting Taxpayer Funds from Mismanagement and Misuse*; *Enhancing Cybersecurity*; *Ensuring Effective and Efficient Law Enforcement*; and *Restoring Confidence in the Integrity, Fairness, and Accountability of the Department*. While we do not prioritize the challenges we identify in our annual top management challenges report, we believe that one of the challenges highlighted this year, which we also identified in last year's report, represents an increasingly critical threat to the Department's ability to fulfill its mission. That challenge is *Addressing the Growing Crisis in the Federal Prison System*.

The crisis in the federal prison system is two-fold. First, the costs of the federal prison system continue to escalate, consuming an ever-larger share of the Department's budget with no relief in sight. In the current era of flat or declining budgets, the continued growth of the prison system budget poses a threat to the Department's other critical programs – including those designed to protect national security, enforce criminal laws, and defend civil rights. As I have stated in testimony to Congress during the past year, the path the Department is on is unsustainable in the current budget environment. Second, federal

prisons are facing a number of important safety and security issues, including, most significantly, that they have been overcrowded for years and the problem is only getting worse. Since 2006, Department officials have acknowledged the threat overcrowding poses to the safety and security of its prisons, yet the Department has not put in place a plan that can reasonably be expected to alleviate the problem.

Meeting this challenge will require a coordinated, Department-wide approach in which all relevant Department officials – from agents, to prosecutors, to prison officials – participate in reducing the costs and crowding in our prison system. In that respect, the challenge posed by the federal prison system is reflective of all of the challenges on our list: each is truly a challenge to be addressed by the Department as a whole, not just by individual Department components.

We hope this document will assist the Department in enhancing its operations and prioritizing its efforts to improve. We look forward to continuing to work with the Department to respond to these important issues in the coming year.

Attachment

---

1. Addressing the Growing Crisis in the Federal Prison System

The Department of Justice (Department) is facing two interrelated crises in the federal prison system. The first is the continually increasing cost of incarceration, which, due to the current budget environment, is already having an impact on the Department's other law enforcement priorities. The second is the safety and security of the federal prison system, which has been overcrowded for years and, absent significant action, will face even greater overcrowding in the years ahead.

Containing the Cost of the Federal Prison System

Although the Department's mission has remained substantially unchanged since 2001, the budgetary environment has changed dramatically. After enjoying an increase in its discretionary budget from $21.5 billion in fiscal year (FY) 2001 to $28.9 billion in FY 2011, the Department's discretionary budget decreased in FY 2012 to $28.3 billion, and by 10 percent in FY 2013 to $25.5 billion. During this same period, the prison population in the Federal Bureau of Prisons' (BOP) facilities grew from about 157,000 inmates in FY 2001 to about 219,000 inmates presently. As a result, the cost of the federal prison system has increased dramatically and represents an ever increasing portion of the Department's budget. For example, pre-trial detention costs, which are the responsibility of the U.S. Marshals Service (USMS), were $617 million in FY 2001, but by FY 2013 those costs had more than doubled to $1.5 billion. Similarly, the budget for the BOP, which is primarily responsible for housing sentenced defendants, was $4.3 billion in FY 2001, or about 20 percent of the Department's discretionary budget, but by the end of FY 2013 the BOP's budget had grown to $6.4 billion, or 25 percent of the Department's discretionary budget. Moreover, according to the President's most

recent budget, the total cost of federal correctional activities will continue to rise through at least FY 2018. By that time, if the BOP's budget increases at the same rate projected for all federal correctional activities and the Department's budget remains flat, the BOP's budget will consume over 28 percent of the Department's discretionary budget.

The Department's leadership has noted that these rising prison costs threaten the Department's ability to fulfill its mission in other areas. For example, in a recent speech to the American Bar Association, the Deputy Attorney General remarked that the "unsustainable" cost of the prison system represents "a crisis that . . . has the potential to swallow up so many important efforts in the fight against crime," and that "[e]very dollar we spend at the Department of Justice on prisons and detention . . . is a dollar we are not spending on law enforcement efforts aimed at violent crime, drug cartels, public corruption cases, financial fraud cases, human trafficking cases, [and] child exploitation, just to name a few."

Yet each year the costs of the federal prison system continue to grow, with no evidence that the cost curve will be broken anytime soon. In August 2013, the Attorney General announced a program to limit the number of defendants that face lengthy prison sentences for drug offenses by instructing federal prosecutors not to charge defendants under statutes carrying mandatory minimum sentences if the defendants are nonviolent; do not have significant ties to large-scale drug trafficking organizations, gangs, or cartels; and do not have significant criminal histories. However, this policy change is unlikely to have a significant short-term impact on prison costs because defendants who qualify for this relief are still likely to face some period of incarceration for their crimes. Whether the policy change will have a material long-term impact on prison costs remains to be seen since many of these same defendants, if they had been subjected to a mandatory minimum charge, might have qualified for the mandatory minimum "safety valve" that Congress created in 1994. This "safety valve" is already incorporated into the federal sentencing guidelines and can result in a sentence of less time in prison than the mandatory minimum sentence specifies.

The Department also introduced in August 2013 the Smart on Crime initiative, which sets out five principles designed to identify reforms to enforce federal laws more fairly and efficiently. Some of these principles echo strategies Department officials have discussed previously, such as pursuing lower-cost alternatives to incarceration for those convicted of low-level, non-violent crimes, including drug courts and diversion programs. The initiative also directs prosecutors to pursue the most serious cases, based on the Department's priorities to protect Americans from national security threats, violent crime, and financial fraud, and to protect the most vulnerable members of society. It further encourages prosecutors to focus on significant cases rather than just the number of cases prosecuted. The Office of the Inspector General (OIG) is monitoring several issues related to the Department's implementation of the Smart on Crime initiative, including the use of pre-trial diversion and drug court programs.

The Smart on Crime initiative represents a strategy that could help contain federal prison costs depending upon the success of its implementation. The Department's policies governing prosecutorial and investigative decisions are a key driver of prison costs, and they need to reflect the real and growing impact that increasing prison costs are having on the Department's budget. Additionally, prosecutorial and

investigative components should be aware that, in a flat or declining budget environment, increased spending on the prison system has the potential to impact spending on their own activities. The Smart on Crime initiative appears to be an attempt to better align the investigative and prosecutive policies that drive incarceration costs with the Department's current budget situation. However, with the President's most recent budget projecting continually increasing costs for federal correctional activities in the coming fiscal years, and with the Department's own projection that the BOP's prison facilities will suffer even greater capacity challenges in the years ahead as discussed below, it is likely additional steps still will be required in order to address this challenge.

Another growing challenge for the federal prison budget is the increasing number of elderly inmates. From FY 2010 to FY 2013, the population of inmates over the age of 65 in BOP-managed facilities increased by 31 percent, from 2,708 to 3,555, while the population of inmates 30 or younger decreased by 12 percent, from 40,570 to 35,783. This demographic trend has significant budgetary implications for the Department because older inmates have higher medical costs. The National Institute of Corrections has estimated that elderly inmates are roughly two to three times more expensive to incarcerate than their younger counterparts. For example, according to BOP data, in FY 2011, the average cost of incarcerating a prisoner in a BOP medical referral center was $57,962 compared with $28,893 for an inmate in the general population. Moreover, inmate health services costs are rising: BOP data shows that the cost for providing health services to inmates increased from $677 million in FY 2006 to $947 million in FY 2011, a 40 percent increase. The OIG is currently reviewing the trends in the BOP's aging inmate population, the impact of incarcerating a growing population of aging inmates, the effect of aging inmates on the BOP's incarceration costs, and the recidivism rate of inmates age 50 and older who were recently released.

In addressing these issues, the Department must better manage and leverage its existing programs. Recent OIG reviews have identified several such opportunities. For example, in 2011 the OIG reviewed the Department's International Prisoner Treaty Transfer Program, which permits certain foreign national inmates from treaty nations to serve the remainder of their sentences in their home countries. Foreign nationals made up as much as 26 percent of federal inmates as of August 2013, and 46 percent of federal defendants in FY 2012. However, the OIG found in our 2011 report that from FY 2005 through FY 2010, the Department rejected 97 percent of foreign national inmates' requests to transfer, and that in FY 2010, 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 of the factors involved in this outcome were beyond the Department's control, such as the requirement that treaty nations must approve a transfer request before a transfer can be completed, the OIG found that if only 5 percent of eligible inmates who had never previously applied were transferred to their home countries, the BOP would remove 1,974 inmates from its prisons and save up to $50.6 million in annual incarceration costs. However, 2 years after the OIG's report was issued, the Department has not fully implemented the report's recommendations and, although the Department appears to have made improvements to its program, BOP data shows that the number of prisoners transferred from BOP's custody under the program has not significantly increased since our report. At a time when the Department's leadership is concerned about a prison cost crisis, the Department must continue its efforts to improve the

implementation of this program that has been authorized by Congress and that could have a material impact on prison costs.

The BOP's compassionate release program, which allows the Department to release inmates under extraordinary and compelling conditions, also could provide some budgetary relief for the BOP. However, an OIG review earlier this year found that the program was badly mismanaged and that better administration of the program would inevitably result in cost savings to the BOP and help the BOP address its capacity problems. As part of the Department's Smart on Crime initiative, and in response to our review, the BOP has issued a new compassionate release policy that expands the program's medical criteria and also includes criteria for elderly inmates. Similarly, in February 2012, the Government Accountability Office (GAO) assessed the flexibility available to the BOP to reduce inmates' time in prison and found opportunities for improvement, including expanded use of the BOP's Residential Drug Abuse Treatment Program and community confinement at the end of sentences. To have a meaningful impact on its immediate budget situation, the Department needs to consider how it can move forward in all of these areas.

Finally, one of the factors contributing to the increasing number of prisoners in the federal prison system over the past 3 decades has been the trend to prosecute at the federal level many offenses that were previously handled largely or exclusively by state and local authorities. By one estimate, the number of federal criminal offenses grew by 30 percent between 1980 and 2004; indeed, there are now well over 4,000 offenses carrying criminal penalties in the United States Code. In addition, an estimated 10,000 to 100,000 federal regulations can be enforced criminally. In May 2013, the House Committee on the Judiciary passed a bipartisan resolution to create the Over-Criminalization Task Force to review federal laws and modernize the criminal code. The Department should simultaneously consider how the federalization of criminal law has affected its budget and operations, and whether rebalancing the mix of cases charged federally might help alleviate the budget crisis posed by the federal prison system without sacrificing public safety, particularly where state and local authorities have jurisdiction to prosecute the conduct.

Improving Prison Safety and Security

Ensuring the safety of staff and inmates in federal prison and detention facilities is among the Department's most important responsibilities, a fact tragically demonstrated when, in February 2013, an inmate using a homemade weapon murdered a correctional officer at a BOP high security facility. The BOP is responsible for the custody and care of approximately 219,000 federal inmates and detained persons awaiting trial or sentencing. Approximately 81 percent of these individuals are confined in BOP-operated facilities, while the rest are confined in privately managed or community-based facilities and local jails. Yet, as of November 2013, the BOP was operating with its facilities at approximately 36 percent over rated capacity, with medium security facilities operating at approximately 45 percent over rated capacity and high security facilities operating at approximately 51 percent over rated capacity. This overcrowding affects the safety and security of a large and growing number of staff and correctional officers, as well as the inmates themselves.

The Department first identified prison overcrowding as a programmatic material weakness in its FY 2006 Performance and Accountability Report and has done so

again in every such report for the past 7 years. Each year, the Department has created a corrective action plan to address the issue, yet the outlook for the federal prison system has remained bleak: even under the scenario outlined in the Department's plan, which assumes it will be fully funded and implemented in each of the next 5 years, the BOP projects that its system-wide crowding will continue to rise to 44 percent over rated capacity by 2018. The costs of achieving even these results will be significant, as reflected in the Department's FY 2014 budget request, which includes $236.2 million in enhancements to maintain secure facilities, improve prisoner reentry, pay for increased detention-related costs, and fund the initial or continued activation of five facilities that will increase the BOP's rated prison capacity by about 4,600 beds. These enhancements would also cover the addition of 1,000 contracted beds at a cost of $26.2 million.

The growth of the inmate population, along with the Department's tightening budget situation, has prevented the BOP from reducing its inmate-to-correctional officer ratio, which has remained at approximately 10-to-1 for more than a decade. In comparison, the Congressional Research Service reported that among the five largest state correctional systems in 2005 – California, Texas, New York, Florida, and Georgia – the highest ratio of inmates to correctional officers was just over 6-to-1. The Department has indicated it is attempting to address this problem by, among other things, requesting funding for an additional 1,155 correctional officers in FY 2014 as compared to FY 2012 enacted staffing levels. However, in the current budget environment, more funding for the BOP to pay for additional correctional officers may simply result in less money being available for other Department priorities. As a result, the Department also needs to consider addressing the other part of the correctional officer-to-inmate equation, namely the number of federal inmates.

Overcrowding at BOP institutions has a significant financial impact on the USMS. The USMS is projected to detain an average of 62,131 individuals per day in FY 2014, a 15-percent increase since FY 2004. The USMS estimates that the BOP will only be able to house approximately 18 percent of USMS detainees. The USMS must pay to house the remainder – an average of about 50,000 detainees per day – in approximately 1,100 state, local, or private facilities.

There are several other important safety and security issues at federal prison and detention facilities that the OIG is monitoring carefully. The OIG has long been committed to addressing allegations of staff-on-inmate sexual abuse in federal prisons. The *Prison Rape Elimination Act of 2003* (PREA) expanded the Department's responsibility to prevent the sexual abuse of inmates in BOP facilities and detainees in the custody of the USMS. In response to PREA, the OIG has processed over 1,000 complaints related to allegations of sexual abuse and opened criminal cases on over 200 of those complaints. This work by the OIG, which is ongoing, has resulted in numerous criminal convictions and administrative actions by the BOP and the USMS. PREA also required the Department to issue national standards for preventing, detecting, reducing, and punishing sexual abuse in prison, which it did in May 2012. With national standards in place, the Department must ensure that those standards are being met, which will require careful oversight of BOP, USMS, and federal contract facilities, including residential reentry centers, and an extensive program for compliance auditing. The OIG intends to monitor the Department's efforts to ensure that the national standards are met.

The OIG is also conducting oversight to help ensure that the Department takes appropriate and cost-effective measures to keep contraband and weapons out of prisons. For example, as a standard part of our investigations involving the introduction of contraband to BOP facilities, the OIG has begun assessing the implementation and effectiveness of the BOP's employee search policies, which the BOP substantially revised in July 2013. In addition, the OIG is reviewing a $4 million contract the BOP awarded for X-ray scanners used to augment the BOP's efforts to inspect packages entering its facilities. This review will assess the use of the purchased equipment and its effectiveness in meeting the BOP's security needs.

Finally, the Department's efforts to ensure the safety and security of its prison and detention facilities must address the challenges relating to the mental health of its inmates and the impact of correctional approaches such as solitary confinement on inmates' mental health and recidivism rates. For example, a July 2013 GAO report recommended that the BOP improve the timeliness of its internal reviews relating to mental health services, develop a plan to evaluate treatment programs, and update its formal policies related to mental health services. In February 2013, the BOP also stated its intention to hire an independent auditor to assess its use of solitary confinement, and that review is now underway. The OIG intends to monitor the BOP's actions closely, including its responses to the GAO's recommendations and the results of the study of its use of solitary confinement, and will conduct additional work in this area as appropriate.

2. Safeguarding National Security Consistent with Civil Rights and Liberties

According to the Department's Strategic Plan for FYs 2012–2016, defending national security from both internal and external threats remains the Department's top priority, and April's bombings during the Boston Marathon tragically demonstrated the importance of this effort. However, the Department's challenge is not limited to ensuring that its efforts to safeguard American interests are effective: it must also protect civil rights and liberties. Recent disclosures concerning the government's data collection and surveillance processes have sparked public debate over mass surveillance and government secrecy, and in so doing have underscored the difficulty of operating national security programs while also respecting the public's expectations of privacy, a key civil rights and liberties concern.

The Department's national security efforts have long been a priority of the OIG's oversight work, which has consistently shown that the Department faces many persistent challenges in its efforts to 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 Department has made important progress in this regard. For example, in response to OIG audits, the Federal Bureau of Investigation's (FBI) has implemented new policies and procedures to better ensure that the terrorist watchlist is complete, accurate, and current. We are conducting a follow-up audit to assess the effectiveness of the FBI's most recent efforts in this area.

Technological advances, particularly in the realm of communications technology, have vastly increased the amount of data potentially available to law enforcement

agencies, thereby compounding the difficulty of ensuring that relevant information is identified and shared among law enforcement entities in a timely and actionable manner. For this reason and others, information sharing remains a persistent challenge to the Department's efforts to ensure national security. Our recent interim report on the federal Witness Security (WITSEC) Program demonstrated the continuing stakes of this challenge. That review found that the Department did not authorize the disclosure to the Terrorist Screening Center of new identities provided to known or suspected terrorists and their dependents who were admitted into the WITSEC Program. Consequently, it was possible for known or suspected terrorists to use their new government-issued identities to fly on commercial airplanes, thereby evading one of the government's primary means of identifying and tracking terrorists' movements and actions. Improved information sharing would also increase the efficacy of the FBI's Foreign Terrorist Tracking Task Force (FTTTF), which conducts in-depth analyses using government and public source datasets to identify and track terrorist and national security threats and provides intelligence on these threats to the intelligence community. An OIG review found that while the FTTTF provides significant value to the Department by proactively identifying national security threats, it would benefit from better coordination with and outreach to FBI field offices to ensure that relevant and actionable information is provided to the agents who need it in a timely manner.

The OIG will continue its efforts to conduct reviews that improve the effectiveness of the Department's national security efforts. Among other reviews, we are continuing our review of the WITSEC Program and will evaluate the Department's progress in implementing corrective measures in response to the recommendations contained in our interim report. We are also working with the Inspectors General of the Intelligence Community, the Central Intelligence Agency, and the Department of Homeland Security to conduct a coordinated and independent review into the U.S. government's handling of intelligence information leading up to the Boston Marathon bombings. The review is examining the information available to the U.S. government before the Boston Marathon bombings and the information sharing protocols and procedures followed between and among the intelligence and law enforcement agencies. In addition, a recent OIG review of the Department's compliance with certain classification requirements found that the Department had not effectively administered its classification policies and procedures to ensure that information is classified and disseminated in compliance with national security information guidelines. We intend to monitor closely the Department's efforts to implement the 14 recommendations we made in that report to help improve the Department's classification management program and its implementation of classification procedures.

While remaining effective in its national security efforts, the Department must simultaneously remain committed to the principles of compliance with law, transparency, and oversight in its management of classified surveillance and data-collection programs. The importance of these principles was demonstrated by 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. 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. We are now conducting a third review of NSL use to assess the FBI's and the Department's progress in responding to the

recommendations made in our past NSL reports and evaluate the FBI's compliance with NSL requirements following its implementation of corrective measures. The OIG's ongoing reviews also include our third review of the Department's requests for business records under Section 215 of the *Foreign Intelligence Surveillance Act* (FISA), as well as our first review of the Department's use of pen register and trap-and-trace devices under FISA. Although the full versions of our prior reports on NSLs and Section 215 all remain classified, we have released unclassified versions of these reports, and we have requested that the Department and the Office of the Director of National Intelligence (ODNI) conduct declassification reviews of the full classified versions. The results of any declassification review may also affect how much information we will be able to publish regarding our pending reviews when they are complete.

The OIG has also conducted oversight of other programs designed to acquire national security and foreign intelligence information, including the FBI's use of Section 702 of the *FISA Amendments Act* (FAA), which authorizes the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information. The OIG's 2012 review culminated in a classified report released to the Department and to Congress that assessed, among other things, the number of disseminated FBI intelligence reports containing a reference to a U.S. person identity and the FBI's compliance with the targeting and minimization procedures required under the FAA. Especially in light of the fact that Congress reauthorized the FAA for another 5 years last session, we believe the findings and recommendations in our report will be of continuing benefit to the Department as it seeks to ensure the responsible use of this foreign intelligence tool. This report also was included in our request to the Department and ODNI for a declassification review, as was the full, classified version of our 2009 report on the President's Surveillance Program, which described certain intelligence-gathering activities that took place prior to the enactment of the FAA.

Additional concerns about civil rights and liberties are likely to arise in the future. For example, significant public attention has been paid to programs authorizing the acquisition of national security information, but relatively less has been paid to the storing, handling, and use of that information. Yet after information has been lawfully collected for one investigation, crucial questions arise about whether and how that information may be stored, shared, and used in support of subsequent investigations. Similar questions arise about the impact on civil rights and liberties of conducting electronic searches of national security information and about whether and how information obtained in a national security context can be used for criminal law enforcement. As the Department continues to acquire, store, and use national security information, these issues will arise more and more frequently, and the Department must ensure that civil rights and liberties are not transgressed.

3. Protecting Taxpayer Funds from Mismanagement and Misuse

Avoiding wasteful and ineffective spending is a fundamental responsibility of federal agencies in any budgetary environment, but in the current climate of budget constraints the Department needs to take particular care to ensure that it is operating as efficiently and effectively as possible. The OIG's recent oversight work has demonstrated the challenges facing the Department. In FY 2013 alone, the OIG's reports, including those related to audits performed by independent auditors

pursuant to the *Single Audit Act*, identified more than $35 million in questioned costs and more than $4 million in taxpayer funds that could be put to better use. These figures are in addition to the numerous OIG recommendations for program improvements that have not been quantified in dollars, many of which remain open.

The OIG's reports have identified numerous opportunities for improved efficiency at the Department. For example, in a review of Department airfares and booking fees, the OIG found that the Department has not configured its travel booking system to ensure that employees on official travel select the most cost-effective airfare available, and that it can continue to reduce travel contractor fees by maximizing the use of its online booking system. Other recent OIG audits have identified problems with USMS procurement policies and practices. An OIG audit found significant deficiencies in how the USMS Office in the Superior Court of the District of Columbia (SCDC) accounts for overtime and supplemental pay for law enforcement officers; identified over $275,000 in total unsupported costs associated with district-level salaries, fleet cards, and purchase cards; and concluded that the USMS SCDC needs to take multiple actions to strengthen its internal controls to ensure that it is adequately preventing waste, fraud, and abuse. A separate OIG audit of USMS procurement actions found that a substantial portion of the actions we reviewed lacked appropriate and necessary documentation, such as evidence of advance approvals, required certifications of fund availability, receiving documents, or justifications for sole source awards or limited competition. Problems such as these have the potential to undermine the Department's reputation as a trusted custodian of public safety and taxpayer funds.

The Department must remain particularly vigilant when taxpayer funds are distributed to third parties, such as grantees and contractors. In part due to the sheer volume of money and the large number of recipients involved, grant funds present a particular risk for mismanagement and misuse: according to the Administration's USASpending.gov website, from FY 2009 through FY 2013 the Department awarded approximately $17 billion in grants to thousands of governmental and non-governmental recipients. These risks were evident in a recent OIG audit which questioned nearly all of the more than $23 million in grant funds awarded by the Department to Big Brothers Big Sisters of America (BBBSA), which resulted in the Department's Office of Justice Programs (OJP) deciding to freeze the disbursement of all grant funds to BBBSA.

The Department has reported taking important steps toward improving its management of this vast and diverse grantmaking effort. For example, the Associate Attorney General's Office established a Grants Management Challenges Workgroup that is responsible for developing consistent practices and procedures in a wide variety of grant administration and management areas. In January 2012, the Department issued policy and procedures developed by the workgroup to implement the Department-wide high risk grantee designation program, which allows the Department to place additional restrictions on the use of funds it provides to grantees who, for example, are deemed financially unstable or have failed to conform to the terms and conditions of previous awards.

The Department should continue to be aggressive in identifying high risk grantees and placing appropriate restrictions on their funds – or halting their funding altogether. But the Department also has other tools at its disposal to mitigate the risk of releasing funds to grantees, such as ensuring that pass-through agencies that

receive block grants have robust subrecipient monitoring systems, ensuring that grantees have adequate accounting procedures in place to track their use of Department funds, attaching special conditions to grants where grantees may have difficulty complying with Department grant requirements, actively seeking suspension and debarment of grantees in appropriate cases, and making use of tools designed to deter smaller-dollar fraud, such the *Program Fraud Civil Remedies Act*, which can be used for false claims where the alleged liability is less than $150,000.

The Department's grantmaking components must also ensure that their own operations are streamlined to ensure maximum value for the taxpayer. Specifically, recent OIG and GAO reports have found that improvements could be realized by reducing duplication and improving coordination among the Department's three grantmaking components, the Office of Community Oriented Policing Services, the Office on Violence Against Women, and OJP. The Department reported in FY 2012 that it would conduct an assessment to better understand the extent to which the Department's grant programs overlap with one another and to determine if grant programs may be consolidated to mitigate the risk of unnecessary duplication. We have not yet been provided with the results of that planned assessment. The Department should take prompt action to address these concerns, and the OIG will continue to closely monitor the Department's actions in addressing duplicative functions in order to ensure that these grantmaking components are optimally coordinating with each other to ensure the maximum effectiveness of each grant dollar spent.

The Department also plays an important role in protecting taxpayer funds through its efforts to enforce laws against financial offenses and fraud. For example, in FY 2012, the Department reported recoveries of approximately $5 billion in false claims cases – the largest annual recovery in its history – with $3 billion attributable to health care fraud civil recoveries and $1.4 billion attributable to housing and mortgage fraud. The OIG is currently reviewing the Department's efforts to address mortgage fraud, including its policy guidance, coordination of component programs at the national level, and public reporting of mortgage fraud-related accomplishments.

But securing a financial judgment is not enough. The Department must also use all available tools to recover money owed to it, and it must ensure that the recovered money is wisely spent. In FY 2012, the U.S. Attorneys' Offices (USAO) collected $13.2 billion in criminal and civil actions, more than double the amount collected in FY 2011. However, at the end of FY 2012, an additional $23 billion was owed to the United States, including $18 billion in criminal fines and $5 billion in civil debts. The USAOs' efforts to collect criminal and civil debts are the subject of an ongoing OIG review. Of similar significance to the taxpayer, the balance of the Department's Assets Forfeiture Fund, which is funded by law enforcement asset forfeitures, rose from $2.9 billion in FY 2011 to $4.4 billion as of FY 2012. A portion of these funds is available to be shared with state and local law enforcement agencies for permissible law enforcement uses, and from FY 2011 to FY 2012, these "equitable sharing" payments increased from $440 million to $681 million. While this program represents an important opportunity for the Department to collaborate with state and local partners, it also creates an opportunity for abuse, as demonstrated by a recent OIG investigation of a local law enforcement entity that resulted in the recovery of $1.8 million in misused equitable sharing revenues. As a result of this investigation, the Department is revising its policies to prevent similar abuses in the future.

Finally, whistleblowers play a critical role in preventing and rooting out mismanagement, waste, and other abuses in the Department, yet retaliation against whistleblowers by Department employees remains a serious subject of concern. For example, in a report released in May 2013, the OIG found that a then-U.S. Attorney, who had resigned prior to the issuance of our report, violated Department policies by disclosing an internal memorandum to a journalist. We concluded that there was substantial evidence that the U.S. Attorney's motive for disclosing the memorandum was to retaliate against a Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) special agent who had previously testified before a congressional committee regarding his concerns about Operation Fast and Furious. The Department must redouble its efforts to aggressively respond to any attempt to retaliate against whistleblowers.

In light of the importance of whistleblowers to the effective management of the Department, in 2012 the OIG created a Whistleblower Ombudsperson position, one of the first within the federal government, to enable the OIG to continue its leadership as a strong and independent voice within the Department on whistleblower issues, and the OIG was recently certified by the U.S. Office of Special Counsel (OSC) as compliant with training and other whistleblower provisions pursuant to 5 U.S.C. § 2302(c). We believe the Department should consider having its components obtain similar certification from the OSC. The OIG also has been, and will continue to be, actively involved in developing whistleblower-related policies, procedures, and training within the Department; in ensuring that whistleblower complaints are reviewed quickly and thoroughly; and in working with other agencies and OSC to help deter retaliation against whistleblowers. The OIG has provided its staff with training on whistleblower rights and protections using a video developed in conjunction with the Department's Office of Legal Education and Justice Television Network, and we are now working with the Department to ensure that training on this important topic is expanded to other components.

4. Enhancing Cybersecurity

The United States continues to face serious, rapidly evolving national security threat posed by cyber attacks and cyber espionage against its computer systems and infrastructure. The Director of National Intelligence's March 2013 *Worldwide Threat Assessment of the U.S. Intelligence Community* emphasized this threat and noted that digital technologies evolve faster than our ability to understand the security implications and mitigate potential risks. Moreover, the increased pace of attacks is staggering: a recent report by the GAO found that the number of cybersecurity incidents federal agencies reported as having placed sensitive information at risk increased 782 percent from 2006 to 2012, averaging more than 130 incidents per day during FY 2012. These cyber attacks are in addition to the threat posed by more traditional unauthorized disclosures by government employees and contractors, disclosures that are significantly aided by the electronic storage and transmission of increasing amounts of information.

The Department's FY 2014 budget request reflects its continued recognition of cybersecurity as a top priority. The request includes $668 million specifically related to cybersecurity, an increase of $92.6 million, or 16 percent, from FY 2013. The majority of the increase, $86.6 million, is to support the FBI's Next Generation Cyber Initiative, which was launched in 2012 to enhance the FBI's ability to help address cybersecurity threats to the nation and which is the subject of a recently initiated

OIG audit. The increased funding would be used in part to add 50 special agents and 50 computer scientists to increase cyber investigation capabilities and victim identification. As criminals increasingly exploit cyber vulnerabilities and use sophisticated digital technologies and computer networks in the commission of crimes, it is important for the Department and the FBI to ensure that all of its agents – not just those designated as cyber specialists – are properly trained in basic cyber investigatory techniques and provided with adequate cyber tools to conduct their investigations.

As the Department increases its cyber capabilities, coordinating its cyber efforts will become even more important. Within the Department, numerous entities and offices focus on cybersecurity and cybercrime. Among those entities is the FBI's Cyber Division, which leads the Department's cyber investigative efforts as the component responsible for protecting against cyber-based terrorism, espionage, and computer intrusions. But there are many others, including the National Security Division's cyber unit, the Criminal Division's Computer Crime and Intellectual Property Section, and the many USAOs responsible for prosecuting cyber cases. The FBI is also responsible for leading the National Cyber Investigative Joint Task Force, which involves senior personnel from approximately six key federal agencies and which the President has directed to be the central point for all government agencies to coordinate and share information related to domestic cyber threats. This proliferation of cybersecurity efforts creates the pressing challenge of proper coordination to ensure that the Department's cyber efforts work in concert with each other and toward the same goal, and that information related to cyber threats is being properly shared and disseminated.

Importantly, a successful cybersecurity strategy will require cooperation from the private sector, and that cooperation must be reciprocal: not only must the Department conduct sufficient outreach to the private sector and offer sufficient safeguards of private sector proprietary information, it must also be willing to share information about cyber threats so that the private sector can prepare for and defend itself against cyber attacks. To this end, the President issued an Executive Order in February 2013 on Improving Critical Infrastructure Security that required the Department to implement procedures to rapidly share quality cyber threat information with private sector entities. The order stressed increased information sharing from the government to the private sector and the need to ensure that privacy, data confidentiality, and civil liberties protections are in place. The Department should move aggressively to implement the President's order and, in doing so, should ensure that it solicits the input of all key private sector constituents about what information, in what form, would be most useful to receive.

A successful cybersecurity strategy will also need to incorporate measures to combat the use of digital technologies to accomplish intellectual property theft, which the FBI and the Department have identified as a growing threat. The Department's Task Force on Intellectual Property coordinates with federal, state, and local law enforcement partners, and international counterparts, to combat intellectual property crimes, and the Department's 2013 Joint Strategic Plan on Intellectual Property Enforcement identified 26 specific online and off-line actions to protect intellectual property, increase enforcement against counterfeiting networks, and encourage multi-national cooperation to protect rights holders. The Department must take all appropriate actions to combat this threat, including those measures identified in the Administration's Strategy on Mitigating the Theft of U.S. Trade Secrets, issued in

February 2013, which include providing warnings and threat assessments to the private sector on information and technology that are being targeted for theft by foreign competitors and governments.

In addition to preventing, deterring, and responding to cybersecurity incidents, the Department must establish effective internal network defenses to protect its own computer systems and data. Of particular concern are insider threats, and in March 2012 the Department established a working group to create an insider threat prevention and detection program to deter, detect, and mitigate actions by employees and contractors who may represent a threat to national security. The OIG is participating in this working group to ensure, among other things, that suspected incidents of insider threats are appropriately reported to the OIG for possible investigation.

The Department has taken other recent steps to protect its computer systems and data. For example, in August 2013, the Department's Chief Information Officer approved new incident response procedures that include a requirement for the Justice Security Operations Center to notify a subset of Department offices, including the OIG, within 72 hours of significant cybersecurity incidents. These notifications are intended to ensure that determinations regarding breach notifications are made properly and in a timely manner, and to ensure that effective oversight of the Department's response to these breaches is possible. The OIG will actively monitor these notifications to determine whether they require further inquiry or investigation. However, in other areas the Department must do more to help ensure the security of its computer systems and data. For example, the *Federal Information Security Management Act* (FISMA) requires the OIG to perform an annual independent evaluation of the Department's information security programs and practices, which includes testing the effectiveness of information security policies, procedures, and practices of a representative subset of agency systems. The OIG's FY 2012 FISMA audits provided 90 recommendations for improving implementation of the Department's information security program and practices for its computer systems. The Department must address these recommendations promptly, as well as the 42 open recommendations from previous FISMA audits.

5. Ensuring Effective and Efficient Law Enforcement

The Department's traditional law enforcement missions – preventing crime; protecting the American people; and administering justice at the federal, state, local, tribal, and international levels – remain of vital importance and occupy a central place in the Department's current Strategic Plan. The OIG's recent work, however, has identified numerous challenges facing the Department's law enforcement efforts.

A fundamental but persistent challenge in this area is ensuring that each Department law enforcement component has a clear mission and policies that incorporate best practices from across the law enforcement community. The OIG's reviews continue to identify instances in which this does not occur. For example, the OIG's 2012 report on Operations Fast and Furious and Wide Receiver identified significant weaknesses in ATF's ability to conduct adequate oversight of its field offices' firearms trafficking investigations, coordinate with U.S. and Mexican law enforcement entities, and implement public safety controls like those used in other Department law enforcement components. That investigation also determined that ATF and the Department had not devoted sufficient attention to ensuring that ATF's policies

adhered to requirements found in the Attorney General's Guidelines and other Department policies. For example, the Department never amended the Attorney General's Guidelines Regarding the Use of Confidential Informants (the AG Guidelines) to cover ATF after ATF joined the Department in 2003, and ATF did not revise its confidential informant policies to conform to the AG Guidelines until 8 years after ATF joined the Department. In response to these findings, we made a number of recommendations to the Department and ATF, including that the Department maintain a regular working group involving leadership from its law enforcement components to ensure appropriate coordination among them on significant law enforcement policies and procedures, case deconfliction mechanisms, and law enforcement initiatives. The Office of the Deputy Attorney General and ATF have reported to the OIG that they have taken significant actions to address the concerns expressed in our report. The OIG has initiated a follow-up review to evaluate the progress and effectiveness of the measures the Department and ATF have taken to implement the recommendations in our Fast and Furious report, and will consider activities and operations ATF initiated subsequent to the new measures' implementation, including Operation Fearless in Milwaukee. The OIG is also completing two reviews of additional ATF operations along the Southwest Border, one relating to the illegal trafficking of grenade components into Mexico, and the other relating to illegally purchased weapons used at the scene where members of the Los Zetas cartel shot two Immigration and Customs Enforcement agents, one of whom subsequently died.[1]

Additionally, our September 2013 report on ATF's income-generating undercover operations found that ATF did not properly authorize, manage, or monitor these investigations. The OIG found that none of the 35 investigations that had been approved by ATF and the Department fully met ATF's policy requirements for approval. For example, none of the 35 investigations had been reviewed by ATF's Undercover Review Committee as required by ATF policy. We also identified one income-generating undercover operation that did not receive the required prior approvals. Further, ATF misused the proceeds from these investigations and failed to properly account for cigarettes purchased as part of them. Among the problems we found was ATF's inability to reconcile the disposition of 2.1 million cartons of cigarettes with a retail value of more than $127 million. In our recommendations, we again advised the Department that it needed to consider implementing best practices across its law enforcement components for these undercover operations.

The Department also must address issues that affect its investigative and prosecutorial efforts in fundamental ways. One of those challenges is the need to integrate emerging and rapidly evolving technologies into law enforcement efforts even as the legal rules governing those technologies remain in flux. For example, unmanned aerial systems (UAS, or drones), global positioning system (GPS) devices, and mobile phone technologies all promise to improve the efficacy of law enforcement efforts by making locational data more available. But these technologies also raise important civil liberties considerations and as-yet unsettled legal questions about what policies are appropriate for governing their approval and use in law enforcement. A recent OIG review of the Department's domestic use of UAS illustrates the point. During our review, FBI and ATF officials stated that they did not believe there was any practical difference between how UAS and manned aircraft collect evidence through aerial surveillance. However, we found that the technological capabilities of drones – such as their ability to fly for extended periods of time and maneuver effectively yet covertly around residences – and the current,

uncoordinated approach of Department components to using UAS may merit the Department developing consistent UAS policies to guide the proper use of UAS. Similarly, issuing and maintaining appropriate guidance on permissible and recommended law enforcement uses of other emerging technologies, and carefully tracking their use, will help ensure that the Department continues to respect individuals' privacy and ensure the admissibility of evidence in future court proceedings.

A staple of the Department's law enforcement approach has been to provide strong support to state, local, tribal, and international law enforcement efforts, a strategy that aims to capitalize on resources outside the Department. However, creating, coordinating, and supporting partnerships can present unique challenges in Indian Country and the U.S. territories. In Indian Country, where there are disproportionately high violent crime rates, widespread substance abuse, and high rates of domestic violence and sexual assault, and where recent FBI data show that violent crime has increased to more than 20 times the national average on some reservations, the responsibility to patrol more than 55 million acres of land must be shared and coordinated among more than 500 federally recognized tribes. The Department's August 2013 Policy Statement on Tribal Consultation established a formal process for Department components to seek tribal input on Department-initiated policies, regulations, and legislative actions that may affect Indian tribes, and in September 2013, the Department announced almost 200 new awards totaling over $40 million in grants under the Coordinated Tribal Assistance Solicitation. The crime data, however, suggest that the Department must redouble its efforts to assist Native American Tribes in reducing violent crime on reservations.

Similarly, crime rates in the U.S. territories have risen drastically in recent years. In Puerto Rico, for example, a 2011 crime report showed that the homicide rate had reached five times that of the U.S. mainland. Criminal Division data also shows that the U.S. Attorney for the District of Puerto Rico secured more federal public corruption convictions between 2002 and 2011 than any other district in the United States and its territories except for the District of New Jersey. Puerto Rico's 130 federal public corruption convictions in 2011 were more than twice the next highest number of such convictions in any other district that year. Previous OIG audits in Puerto Rico and other Territories also have identified problems with grant management and oversight of sub-recipients. The OIG is currently auditing the Puerto Rico Department of Justice's administration of grant funds, including the adequacy of its processes for meeting grant goals and objectives.

As part of its law enforcement mission, the Department must also ensure the efficacy and integrity of its regulatory compliance programs, which are crucially important to preventing crime and ensuring that weapons and hazardous materials are handled, transferred, and stored safely and securely. Recent OIG reviews of ATF's federal firearms licensee and federal explosives licensee inspection programs, however, documented needed improvements to these important efforts. Further, the OIG's recent review of ATF's actions in revoking a firearms license concluded that an ATF field division did not comply with ATF's administrative action policy or instructions it received from headquarters. The OIG will continue its close oversight of law enforcement programs, including through an ongoing review of the Drug Enforcement Administration's adjudication of registrant actions it has taken against businesses or health care practitioners found to have violated the *Controlled Substances Act of 1970*, and through a separate ongoing review of the Department's

process for referring individuals denied the purchase of a firearm by the National Instant Criminal Background Check System to ATF for investigation and possible prosecution.

Finally, the Department's law enforcement components and criminal prosecutors must strive to coordinate and share information and resources as effectively as possible. Information sharing in the criminal context can raise important questions about due process and civil rights, such as when it is appropriate in a criminal investigation to use foreign intelligence information that reveals potential criminal activity of American citizens, and how the use of such information will affect a subsequent prosecution. The OIG is conducting multiple reviews relating to information sharing among law enforcement agencies, including the previously mentioned multiagency review of the U.S. government's handling of intelligence leading up to the Boston Marathon bombings and a review of the Organized Crime Drug Enforcement Task Forces Fusion Center.

6. Restoring Confidence in the Integrity, Fairness, and Accountability of the Department

Public trust in the Department, its senior officials, and its employees is essential to every aspect of the Department's operations. The Department must ensure that it strengthens and maintains its reputation for integrity, fairness, and accountability of its personnel and its operations.

The non-ideological, non-partisan enforcement of law is fundamental to the public's trust in the Department. Yet in a recent report assessing how the enforcement priorities of the Voting Section of the Civil Rights Division have changed over time and whether the voting rights laws have been enforced in a non-discriminatory fashion, the OIG identified issues in the handling of a small number of cases that the OIG believed risked undermining public confidence in the non-ideological enforcement of the voting rights laws. The investigation also revealed several incidents in which deep ideological polarization fueled disputes and mistrust that harmed the functioning of the Voting Section, including numerous examples of harassment and marginalization of employees and managers due, at least in part, to their perceived ideological or political beliefs. These incidents received substantial public attention through congressional hearings and media reporting, thereby feeding the concern that the administration of justice had become politicized. The OIG will monitor the Department's corrective actions taken in response to our report.

The OIG has identified recent instances in which Department employees made inaccurate or incomplete statements to Congress or other government entities. These inaccurate and incomplete statements generated significant attention in both Congress and the national media and resulted in an erosion of trust in the Department. For instance, in the Fast and Furious report referenced above, the OIG found that senior Department and ATF officials shared responsibility for providing inaccurate information in two letters to Congress. The OIG also raised concerns about subsequent representations to Congress by Department officials about Operation Fast and Furious.

Additionally, in September 2013, the OIG released a report finding inaccuracies among terrorism-related statistics that the Executive Office for United States

Attorneys (EOUSA) reported to Congress and the public. These statistics had been used to make operational and budgetary decisions. The report further found that EOUSA had not significantly improved its reporting of terrorism-related statistics since a 2007 audit report that made similar findings. By contrast, the OIG's September 2012 report examining the reporting of terrorism-related statistics by the Department's National Security Division (NSD) found that NSD had improved on the weaknesses identified in our 2007 report but still required additional improvements to ensure the accuracy of reported statistics.

The OIG's investigations of Department employees and contractors during FY 2013 led to 77 criminal indictments or informations resulting in 63 convictions, pleas, or pre-trial diversions. These investigations also prompted 266 administrative disciplinary actions by Department components and resulted in monetary recoveries totaling more than $14.1 million, which includes civil and criminal penalties, judicial and non-judicial fines, forfeitures, and restitution. Investigations by Department components led to additional criminal charges and administrative disciplinary actions. Given that the Department has approximately 115,000 employees, these figures do not indicate widespread abuse and corruption in Department operations, but they do demonstrate the need for continued vigilance and for a robust, fair, and transparent disciplinary process.

For that reason, the OIG has conducted several reviews in recent years that assess the disciplinary systems of the Department's law enforcement components and made recommendations for improvement. Many of these recommendations were designed 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 systems: 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. Accordingly, the OIG is continuing its work with a review of the disciplinary system used by the USAOs and EOUSA, and we have initiated two multi-component reviews, one of how law enforcement components handle sexual misconduct, and another of the Department's efforts to prevent misconduct by employees on official travel or assignment in foreign countries.

Finally, an issue that the OIG has consistently identified as affecting the public's confidence in the Department's efforts to address employee misconduct is the statutory limitation on the OIG's jurisdiction to handle allegations of misconduct by attorneys. Whereas the OIG is the primary oversight entity with respect to most Department employees, including all of its law enforcement agents, the Office of Professional Responsibility (OPR) is authorized by statute to investigate allegations of misconduct against Department attorneys where the allegations relate to the exercise of the attorney's authority to investigate, litigate, or provide legal advice. The OIG has long questioned this distinction between the treatment of misconduct by attorneys acting in their legal capacity and misconduct by other Department employees, including agents. We believe the institutional independence of the OIG, which is codified in the *Inspector General Act*, is critical to the effectiveness of our misconduct investigations. Unlike the OIG, OPR does not have that statutory independence, and the Attorney General appoints and can remove OPR's leader. Additionally, the OIG's strong record of transparency is vital to ensuring the Department's accountability and enhancing the public's confidence in

the Department's operations. For these reasons, we continue to believe that Congress should eliminate this carve-out from the OIG's jurisdiction.

[1]↑ The original version of this report, which was released publicly on December 13, 2013, incorrectly stated that the illegally purchased weapons "were recovered at the scene of the murder of two Immigration and Customs Enforcement agents." In fact, two agents were shot, one subsequently died, and the weapons were recovered several days later and tied to the shootings using forensic and testimonial evidence.