Top Management and Performance Challenges Facing the Department of Justice - 2014

November 10, 2014

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 2014 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 seven challenges that we believe represent the most pressing concerns for the Department. They are *Addressing the Persisting Crisis in the Federal Prison System*; *Safeguarding National Security Consistent with Civil Rights and Liberties*; *Enhancing Cybersecurity in an Era of Ever-Increasing Threats*; *Effectively Implementing Performance-Based Management; Ensuring Effective and Efficient Oversight of Law Enforcement Programs*; *Upholding the Highest Standards of Integrity and Public Service*; and *Protecting Taxpayer Funds from Mismanagement and Misuse*. While the challenges are not presented in a priority order, we believe the federal prison crisis, safeguarding national security, and enhancing cybersecurity are challenges in three critical areas that will continue to occupy much of the Department's attention and require its sustained focus for the foreseeable future.

In addition, one of the challenges, *Effectively Implementing Performance-Based Management*, offers the Department the opportunity to realize improvements and positive results across the spectrum of its programs and operations. Meeting this challenge will require the Department to use accurate and reliable data, develop results-oriented measurements, and adopt a data-driven analytical approach in its evaluation of program performance. We recognize that achieving results-oriented measurement is particularly difficult in areas such as litigation and law enforcement, but it is of critical importance if the Department is to effectively monitor whether its programs are accomplishing their intended goals. Performance-based management will enhance the Department's ability to achieve its strategic management objectives and address its most salient challenges.

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

Attachment.

---

1. Addressing the Persisting Crisis in the Federal Prison System

The Department of Justice (Department) continues to face two interrelated crises in the federal prison system. First, despite a slight decrease in the total number of federal inmates in fiscal year (FY) 2014, the Department projects that the costs of the federal prison system will continue to increase in the years ahead, consuming a large share of the Department's budget. Second, federal prisons remain significantly overcrowded and therefore face a number of important safety and security issues.

Containing the Cost of the Federal Prison System

The costs to operate and maintain the federal prison system continue to grow, resulting in less funding being available for the Department's other critical law enforcement missions. Although the size of the federal prison population decreased for the first time since 1980, from 219,298 inmates at the end of FY 2013 to 214,149 inmates at the end of FY 2014, and the Department now projects that the number of inmates will decrease by 10,000 in FY 2016, the downward trend has yet to result in a decrease in federal prison system costs. For example, in FY 2000, the budget for the Federal Bureau of Prisons (BOP) totaled $3.8 billion and accounted for about 18 percent of the Department's discretionary budget. In comparison, in FY 2014, the BOP's enacted budget totaled $6.9 billion and accounted for about 25 percent of the Department's discretionary budget. During this same period, the rate of growth in the BOP's budget was almost twice the rate of growth of the rest of the Department. The BOP currently has more employees than any other Department component, including the Federal Bureau of Investigation (FBI), and has the second largest budget of any Department component, trailing only the FBI. The Department's leadership has acknowledged the dangers the rising costs of the federal prison system present to the Department's ability to fulfill its mission in other areas. Nevertheless, federal prison spending continues to impact the Department's ability to make other public safety investments, as the Department's FY 2015 budget request for the BOP is a 0.5 percent increase from the enacted FY 2014 level.

Our work has identified several funding categories where rising prison costs will present particularly significant challenges in future years. For example, inmate healthcare costs constitute a rapidly growing portion of the federal prison system budget. According to BOP data, the cost for providing healthcare services to inmates increased 55 percent from FY 2006 to FY 2013. The BOP spent over $1 billion on inmate healthcare services in FY 2013, which nearly equaled the entire budget of the U.S. Marshals Service (USMS) or the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). The rapid increase in inmate healthcare costs can partly be

attributed to the growth of the aging inmate population. From FY 2009 to FY 2013, the population of sentenced inmates age 50 and over in BOP-managed facilities increased 25 percent, while the population of sentenced inmates under the age of 30 decreased by 16 percent. The growth in the aging inmate population has significant budgetary implications for the Department because, according to studies cited by the National Institute of Corrections in a 2004 report, older inmates generally cost more than their younger counterparts to incarcerate. BOP data indicates that aging inmates account for about 19 percent of the total current population in BOP-managed facilities and 31 percent of inmates housed in BOP medical centers. In 2013, the average cost of incarcerating an inmate in a BOP medical center was $58,956 compared to $27,549 for inmates in the general population. The Office of the Inspector General (OIG) is completing a review of the impact of the BOP's aging inmate population on inmate and custody management, including inmate programs and activities, housing, and costs.

The cost of prescription drugs is also driving BOP's healthcare costs. New prescription drug treatments, particularly for chronic hepatitis C (HCV), could exponentially increase costs in the coming years. The BOP currently spends $6,600 per patient for a standard HCV treatment regimen. However, the treatment regimen newly approved by the Food and Drug Administration could cost an additional $20,000 to $40,000 per patient, according to BOP estimates. In 2014, the BOP estimated that at least 11,000 of its inmates have HCV, meaning that the BOP could face additional costs for these patients of approximately $220 million to $440 million. The BOP recently issued interim guidance on the implementation and management of HCV treatments. The OIG continues to monitor the effects of rising healthcare costs.

Given this crisis in the prison system, the Department needs to better utilize programs that can assist in prison population management, particularly existing programs and policies that Congress has already authorized. The OIG found in its 2013 review of the BOP's Compassionate Release Program that the program was not well-run and that an effectively managed program could assist the BOP with its prison capacity issues, which would result in cost savings for the BOP. Following our review, the BOP expanded its Compassionate Release Program to include criteria for elderly inmates with and without medical conditions. Similarly, in our 2011 review of the Department's International Prisoner Transfer Program, which permits certain foreign national inmates from treaty nations to serve the remainder of their sentences in their home countries, the OIG found that the Department rejected 97 percent of transfer requests by foreign national inmates, and that in FY 2010 few foreign inmates were transferred back to their home countries. Following our review, the BOP took steps to ensure that the treaty transfer program was communicated more effectively to inmates. According to recent BOP data, the number of inmates requesting transfer has increased significantly; however, the number of foreign inmates ultimately transferred to their home countries remains stagnant. The OIG anticipates completing its follow-up review of the treaty transfer program this fiscal year, and plans to report on whether there is additional progress that can be made to reduce prisoner numbers and costs in this area.

Separately, the Department has recently announced initiatives and changes in prosecution, sentencing, and early release policies that could reduce federal prison costs. These proposed policies target inmates sentenced for drug offenses, a group that accounts for more than half of the current federal prison population. The

Department's FY 2015 budget request includes $173 million to support the Smart on Crime initiative, which the Department indicates is intended to promote prevention and reentry programs, such as drug courts and veterans courts as alternatives to incarceration, and encourages prosecutors to draft criminal charges for low-level nonviolent drug offenders in ways that will not trigger mandatory minimum sentences. Further, in April 2014, the Department announced a clemency initiative for prisoners already serving long sentences for low-level, non-violent drug offenses.

The Department also has indicated its support for programs that provide alternatives to incarceration, coupled with treatment and supervision, in an attempt to reduce recidivism. In an August 2013 speech, the Attorney General identified state-sponsored initiatives that he said served as effective alternatives to incarceration by providing offenders the treatment and supervision designed to reduce recidivism while also reducing states' prison populations. The Attorney General also instructed all U.S. Attorneys' Offices (USAOs) to designate a Prevention and Reentry Coordinator in their respective Districts to expand on existing programs that promote the implementation of the Smart on Crime initiative. The OIG is currently conducting an audit that will evaluate the design and implementation of pre-trial diversion and drug court programs, variances in the usage of the programs among the USAOs, and costs savings associated with successful program participants.

Improving Prison Safety and Security

At the same time it focuses on prison costs, the Department must continue its efforts to ensure the safety and security of staff and inmates in federal prison and detention facilities. Prison overcrowding presents the most significant threat to the safety and security of BOP staff and inmates. In its FY 2013 Agency Financial Report, the Department once again identified prison overcrowding as a programmatic material weakness, as it has done in every such report since FY 2006. Yet, the federal prisons remain almost as crowded today as they were in FY 2006. As of June 2014, federal prisons operated at 33 percent overcapacity, with 42 percent overcrowding at higher security facilities and 40 percent at medium security facilities. Overcrowding in the federal prison system has prevented the BOP from reducing its inmate-to-correctional officer ratio, which according to the Congressional Research Service has remained at approximately 10-to-1 for more than a decade. The Department's FY 2014-2018 strategic plan includes an outcome goal to reduce system-wide crowding in federal prisons to 15 percent by FY 2018. However, as of June 2014, the BOP's Long Range Capacity Plan projects prison overcrowding to be 38 percent by FY 2018, higher than it is today. To reach the long-term outcome goal in the strategic plan, without expending additional funds to build more federal prison space or to contract for additional non-federal bed space, the Department would have to achieve a net reduction of about 23,400 federal prisoners from the June 2014 prison population, based on the existing bed space available within the federal prison facilities.

The safe and secure incarceration of federal inmates not only applies to BOP-managed facilities, but also extends to privately managed BOP contract facilities. Effective oversight of these facilities is critical since the proportion of inmates housed in contract facilities has increased substantially, from 2 percent of the prison population in 1980 to 19.5 percent in 2013. Riots in two privately managed BOP contract facilities, one in Texas in 2009 and the other in Mississippi in 2012, resulted in the death of a correctional officer, severe injuries to prisoners and employees, and over $60 million in property damage. The causes of both incidents

have been at least partially attributed to prisoners' reactions to their perceptions of inadequate medical conditions and mistreatment at the facilities. The OIG is examining how the BOP manages its private contract prisons, whether the three contract prisons we are reviewing meet BOP and other safety and security requirements and how contract facilities compare with similar BOP facilities in terms of inmate safety and security. The use of segregated housing in private contract facilities and federal prisons also raises inmate safety and security concerns. In 2013, the BOP agreed to have an independent assessment conducted on its use of segregated housing. The OIG awaits the results of the report, and will continue to monitor the BOP's management of restrictive housing operations.

Sexual abuse in prison also remains a serious safety and security issue for the Department. In May 2014, the Department estimated that four percent of state and federal prison inmates reported experiencing one or more incidents of sexual victimization by another inmate or a facility staff member within the previous 12 months. 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. The OIG recently completed a review of the Department's efforts to implement and comply with PREA since the Department's 2012 publication of the National Standards to Prevent, Detect, and Respond to Prison Rape (standards), which apply to all federal, state, and local confinement facilities. The OIG found that while the Department has made progress complying with the standards during the early period of implementation, significant work remains. For example, the Department does not have an effective mechanism in place to ensure compliance with the provisions of the standards that place obligations on the Department's law enforcement components that investigate sexual abuse in confinement settings. Consistent with those standards, all OIG investigators responsible for investigating sexual abuse allegations completed training earlier this year. The OIG will continue its longstanding efforts to investigate allegations of sexual abuse in federal prisons and detention facilities, work that has resulted in numerous criminal convictions and administrative actions by the BOP and the USMS.

The introduction of weapons and contraband, such as drugs, cell phones, and tobacco, into correctional facilities also presents considerable safety and security concerns. The OIG released an audit in June 2014 that assessed the usage and effectiveness of 65 x-ray machines purchased by the BOP for approximately $4 million following an attempted smuggling incident at the Federal Correctional Complex in Pollock, Louisiana. Our audit found that the machines were not effective for screening certain commodities commonly received by institution warehouses, and that prior to the audit the BOP had no policy guidance outlining the x-ray machines' limitations on effectively scanning dense items. In response to an OIG memorandum, the BOP issued guidance to ensure consistent application of all critical security and operational procedures for the use of x-ray machines at all BOP institutions that have received the equipment.

The unauthorized use of cell phones in prisons and detention facilities has proven to be a significant danger, and presents an increasing threat to the safety of the public as well as BOP staff and inmates. According to a 2011 Government Accountability Office (GAO) report, the number of cell phones BOP confiscated at federal prisons increased from 1,774 in 2008 to 3,684 in 2010. BOP officials reported that contraband cell phone use can threaten the security of prisons and expand criminal

activity both inside and outside of prisons. For example, in January 2011 an inmate at a federal institution was sentenced to an additional 14 years in prison for running an identity-theft ring using a contraband cell phone, resulting in over $254,000 in fraudulent purchases. In September 2014, five correctional officers from the Baltimore City Detention Center, which is a state operated facility that also houses federal inmates under a contract with the USMS, pled guilty to participating in a 2-year racketeering conspiracy that included the smuggling of drugs and contraband, including cell phones, for further distribution by inmates who were active gang members. The OIG will continue to monitor cell phone interdiction efforts by the states and the BOP. In July 2013, the BOP released new staff entrance and search procedures, which authorized random pat searches of staff and in September 2014 the BOP announced a pilot program to use Millimeter Wave Scanners (similar to those used in airports) for contraband detection at six institutions. The OIG continues to monitor the BOP's compliance with a 2003 OIG recommendation regarding the searching of staff and their property when entering BOP institutions. In October 2014, the OIG initiated a review of the BOP's contraband interdiction efforts, including staff and visitor searches as well as physical security measures. That review will also examine state prisons' contraband interdiction practices.

Addressing the challenge of ensuring the safety and security of correctional officers and federal inmates will require the BOP to take several actions. First and foremost, the BOP must pursue strategies to reduce prison overcrowding. It must also provide effective oversight of privately managed contract prison facilities, reduce the incidence of inmate sexual abuse, and prevent the smuggling of weapons and contraband into prison.

2. Safeguarding National Security Consistent with Civil Rights and Liberties

The top priority in the Department's FY 2014-2018 strategic plan continues to be protecting U.S. citizens against acts of terrorism. As demonstrated by recent acts perpetrated by the Islamic State of Iraq and the Levant (ISIL) in the Middle East and last year's bombing of the Boston Marathon, the threat posed by terrorism remains serious. The proposed FY 2015 budget for the Department allocates over $4.3 billion to national security efforts to maintain counterterrorism and counterespionage programs and sustain intelligence gathering and surveillance capabilities. Given the potential magnitude of the threat posed, it is particularly important that the Department ensure that these funds are spent wisely, and that they are effective in improving national security. At the same time, however, the Department must ensure that it respects the civil liberties of American citizens. The recent debate over the government's surveillance programs has drawn significant attention to the challenge of operating critical national security programs consistent with the public's expectation of privacy.

The Department's national security efforts continue to be a focus 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 necessary information to act in a timely and effective manner. Our joint review with three other Inspectors General of the government's handling and

sharing of information prior to the Boston Marathon bombings found that the FBI, Central Intelligence Agency (CIA), Department of Homeland Security, and National Counterterrorism Center generally shared information and followed procedures appropriately. Although we found that the FBI did not coordinate with the CIA in 2011 after receiving lead information about one of the alleged perpetrators of the bombings, we concluded that the CIA's involvement likely would not have been helpful to the FBI at that time. We also found that the FBI did not share this lead information with its state and local partners on the Joint Terrorism Task Force prior to the bombings, and we recommended that the FBI consider establishing a procedure for sharing threat information with state and local partners more proactively and uniformly. To identify potential gaps in information sharing that could compromise the effective targeting and disruption of international terrorist groups we intend to conduct a review of domestic information sharing among federal, state, and local law enforcement agencies.

We also continue to review the Department's use of the various investigative tools that it has available to enhance its national security efforts. For example, we are currently examining the Drug Enforcement Administration's (DEA) use of administrative subpoenas to obtain or exploit broad collections of "bulk" data or information. In particular, this review will address the legal authority for the acquisition and use of these data collections.

Various investigative methods used by the Department and the FBI to carry out their national security missions contain safeguards designed to protect the civil liberties of Americans. The importance of achieving the appropriate balance between effective national security efforts and respect for civil liberties and privacy interests was demonstrated by OIG reviews that have assessed the FBI's use of National Security Letters (NSL), which give the government authority to obtain information such as telephone and financial records from third parties without a court order, provided certain requirements are met. The OIG's initial two NSL 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. In our most recent review of the FBI's use of NSLs published earlier this year, we found that the FBI and the Department have devoted considerable resources toward implementing the recommendations made in our past reports, and are taking additional measures to improve the FBI's compliance with NSL requirements. However, we identified additional challenges in certain areas during our compliance review, and we therefore made 10 new recommendations to the FBI and the Department to further improve the use and oversight of NSLs.

Ongoing OIG work, such as our reviews of the Department's requests for and use of business records under Section 215 of the USA PATRIOT Reauthorization Act and the Department's use of pen register and trap-and-trace devices under the Foreign Intelligence Surveillance Act (FISA), also address privacy concerns implicated by the use of national security authorities to collect data. Although the OIG completed both of these reviews months ago, and we have provided classified briefings to Congress regarding them, we have been unable to release the classified reports to Congress or non-classified reports to the public because the classification review being conducted by the intelligence community, which includes the FBI, is still ongoing. Similarly, in 2013, we requested that the Department and the Office of the Director of National Intelligence (ODNI) conduct declassification reviews for the full classified versions of

our prior Section 215 reports, as well as our reports on the President's Surveillance Program and the FBI's use of Section 702 of the FISA Amendments Act, so that these reports can be released publicly. Our requests for the declassification reviews remain pending. We had made a similar request regarding our prior NSL reports and, in October 2014, we released new versions of those prior NSL reports with additional information unredacted after the information was declassified by the Department and ODNI in response to a Freedom of Information Act (FOIA) lawsuit. We believe it is important for the Department and ODNI to promptly review the remaining OIG national security reports that we identified in 2013 for declassification review.

The OIG also is currently reviewing the FBI's use of information derived from the National Security Agency's (NSA) collection of telephony metadata obtained from certain telecommunications service providers under Section 215. The review will examine the FBI's procedures for receiving, processing, and disseminating leads the NSA develops from the metadata, and any changes that have been made to these procedures over time. The review will also examine how FBI field offices respond to leads generated from this collection, and the scope and type of information field offices collect as a result of any investigative activity that is initiated. In addition, the review will examine the role the leads have had in FBI counterterrorism efforts.

The Department must couple its protection of national security with a commitment to the principles of transparency, oversight, and compliance with the law in its management of surveillance and data collection programs. Technological advances have increased the amount of data potentially available for use by law enforcement agencies, and Americans are engaged in a discussion about the value of the information collected and the appropriateness of collection techniques employed under surveillance authorities. New and emerging national security threats continue to drive the Department's work, and as the Department continues to acquire, store, and use information for its national security investigations and prosecutions, concerns about privacy rights and liberties will continue to arise.

3. Enhancing Cybersecurity in an Era of Ever-Increasing Threats

The United States continues to face serious, rapidly evolving economic and national security threats posed by cyber attacks and cyber espionage against its computer systems and infrastructure. In a January 2014 poll conducted by Defense News, leaders in national security policy, the military, Congress, and the defense industry identified cyber warfare as the number one threat facing the United States. In November 2013, FBI Director James B. Comey testified before the Senate Committee on Homeland Security and Governmental Affairs that in the future the resources devoted to cyber threats had the potential to eclipse resources devoted to non-cyber based terrorist threats. As recent events have shown, significant data breaches have occurred in the private sector, including at some of the nation's largest companies. These breaches have exposed to harm the personal data and financial information of millions of Americans. The federal government is also a frequent target of cyber attacks.

The Department has assigned numerous offices responsibility for meeting the cybersecurity challenge. These include the FBI's Cyber Division, which leads the Department's cyber investigative efforts; 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 Cyber Division is responsible for protecting against cyber-based terrorism, espionage, and computer intrusions, and also leads the National Cyber Investigative Joint Task Force (NCIJTF), which is the focal point for coordinating, integrating, and sharing information on cyber threat investigations across 19 U.S. agencies and foreign partners. As we stated in last year's management challenges report, this increasing proliferation of cybersecurity events creates pressing challenges for the Department to properly coordinate its cyber resources to work in concert toward the same goal, and to ensure that information related to cyber threats is shared and disseminated in an appropriate manner.

Moreover, the Department's FY 2015 budget request reflects its continued recognition of cybersecurity as a top priority. The Department requested $722 million, an increase of $7.6 million, to confront computer intrusions and cybercrimes and protect the Department's information networks. Over the last two years, the Department has requested $100.2 million to address rapidly changing cyber threats. The majority of this increase, $86.6 million (and 152 positions), is to support the FBI's Next Generation Cyber Initiative (NGC), which was launched in 2012 to enhance the FBI's ability to address cyber security threats to which the United States is vulnerable. NGC goals include increased partnering with the NCIJTF, focusing cyber security resources on computer and network intrusions instead of crimes committed with a computer, expanding the capabilities of Cyber Task Forces in each of the FBI's 56 Field Offices, and bolstering the FBI's cyber workforce and support infrastructure. The OIG is currently reviewing the NGC Initiative, determining whether the FBI is meeting its goals and assessing the FBI's progress following our 2011 report on its ability to address the national security cyber threat.

In its efforts to combat cybercrimes that impact the private sector, the Department must conduct sufficient outreach. 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. In last year's management challenges report, we stressed the need for the Department to aggressively implement the President's February 2013 Executive Order that requires the Department to implement procedures to rapidly share quality cyber threat information with private sector entities. A response from the Department came recently when the FBI established the Key Partnership Engagement Unit. The new unit aims to share "sector specific threat information" with private sector partners, and has provided classified briefings to key industries including energy and financial services. To avoid duplication, when sharing information with the private sector, the Department must coordinate with other federal agencies performing similar tasks, such as the Department of Homeland Security and the Secret Service. A successful cybersecurity strategy requires cooperation from the private sector, as well as reciprocal cooperation from law enforcement. The OIG will continue to monitor the Department's outreach to the private sector.

In protecting its own computer systems and data, the Department must establish and maintain effective internal network defenses. Of particular concern are insider threats. As recent events have shown, employees and contractors who have access to government computer systems and information in order to do their work, may pose serious security risks from within. In February 2014, the Department established an Insider Threat Prevention and Detection Program. The purpose of this program is to use counterintelligence, security, information assurance, and other

functions and resources to identify and counter insider threats. The Department's Insider Threat Working Group is responsible for the development of minimum standards and guidance for implementing the program, and ensuring that civil liberties issues are adequately addressed.

Further, it is critical that the Department respond to cybersecurity incidents in a timely and meaningful manner. According to the National Institute of Standards and Technology (NIST), organizations need an incident response capability to enable them to detect incidents quickly, minimize loss and destruction, mitigate the system weaknesses that were exploited, and restore information technology services. However, an April 2014 GAO report analyzed a statistical sample of fiscal year 2012 cyber incidents across 24 federal agencies, including the Department, and estimated that the agencies did not effectively or consistently demonstrate actions taken in response to approximately 65 percent of detected incidents. Regarding Department policies and procedures, the GAO report identified several instances where the Department was in full or partial compliance, and in one instance in noncompliance, with key elements defined by the NIST. The report also found that the Department only partially defined the roles, responsibilities, and levels of authority for responding to cybersecurity incidents and did not develop and document procedures for prioritizing incidents. The GAO did, however, note that the Department was the only one of the six federal agencies selected for the audit that had established incident response performance measures.

In an era of ever-increasing cyber threats, the Department will be challenged to sustain a focused, well-coordinated cybersecurity approach for the foreseeable future. The Department must continue to emphasize protection of its own data and computer systems, while marshalling the necessary resources to combat cybercrime and effectively engaging the private sector.

4. Effectively Implementing Performance-Based Management

A significant management challenge for the Department is ensuring, through performance-based management, that its programs are achieving their intended purposes. In a September 2014 speech on criminal justice reforms aimed at reducing the federal prison population and its costs, the Attorney General stated, "it's time to shift away from old metrics and embrace a more contemporary, and more comprehensive, view of what constitutes success … because what gets measured is what gets funded and what gets funded is what gets done." Currently, the Department's 40 components have about 500 performance measures for programs with varied goals that include preventing terrorism and promoting national security, reducing violent crime, enforcing federal laws, and ensuring the fair and efficient administration of justice. Establishing annual and long-term performance measures with ambitious targets is a challenge for many of the Department's programs given that the programmatic outcomes are frequently not easily measured. However, the Department's ability to accomplish its strategic goals is significantly aided by how well it can gather and use data to evaluate program performance and improve management decisions; in addition, empirical evidence can assist in resource allocations and in requesting budget proposals.

Performance-based management has been a long-standing challenge not only for the Department but across the entire federal government. The Government Performance and Results (GPRA) Modernization Act of 2010 updated the federal

government's performance management framework. The Act and corresponding guidance in the Office of Management and Budget's Circular No. A-11 place a heightened emphasis on priority-setting, cross-organizational collaboration to achieve shared goals, and the use and analysis of goals and measurements to improve outcomes. The Act established the website Performance.gov to serve as a single platform to communicate government-wide and agency performance. The Act also requires that federal agencies establish priority goals and cross-agency goals; conduct quarterly data-driven reviews to measure performance in achieving these goals; and use Performance.gov as a vehicle to report this information to the public. These quarterly data-driven performance reviews are modeled after successful evidence-based practices used in both the private and public sectors, such as the New York City Police Department's use of "CompStat" in the early 1990s to reduce crime and improve police performance.

The Department has taken actions to implement the tenets of performance-based management. For instance, in March 2014, the Department developed four agency priority goals to reflect the Attorney General's stated priorities and align with the Department's new strategic plan for FYs 2014-2018. The priority goals address themes concerning national security, violent crime, protecting vulnerable people, and financial and healthcare fraud, and focus on results that can be accomplished over a 12 to 24 month timeframe. Through Performance.gov, the Department has begun to report on a quarterly basis its progress in meeting these goals with performance data. Similarly, the Department developed a new set of key performance measures to track its progress in accomplishing the 30 long-term outcome goals in its new strategic plan. Also, starting in FY 2013, the Department combined its annual performance report and annual performance plan to provide a more useful and integrated picture of the Department's performance.

As the Department implements the GPRA Modernization Act requirements, it must continue its efforts to develop meaningful outcome-oriented goals and performance metrics. Some of the Department's performance goals and indicators are focused on inputs, workload, or processes rather than on outcomes and results. For example, several of the performance measures for the USAOs, such as the number of matters handled or total judgments and settlements, are output rather than outcome focused. These measures may provide information about the number of cases being handled, but they do not assess the significance and impact of those cases, nor do they address the goals of the Smart on Crime initiative. Given the significant role federal prosecutors play in combating crime, serving justice, and keeping the public safe, meaningful and outcome-based USAO performance measures can serve as powerful incentives to allocate resources and ensure focus toward achieving priorities. Achieving results-oriented measurement is particularly difficult in areas such as litigation and law enforcement, but of critical importance if the Department is to effectively monitor whether its programs are accomplishing their intended goals.

Further, Department leadership has acknowledged that the Department needs to embrace data in its evaluation of program performance, such as through advanced data analytics. Adopting a data-driven, analytical approach will be especially important for assessing the implementation of the Attorney General's Smart on Crime initiative. As noted previously, the rising cost of incarceration threatens the Department's ability to fulfill its mission in other priority areas. Much of the Smart on Crime initiative promotes the increased use of prevention and reentry programs, such as the expanded use of pre-trial diversion and drug court programs as

alternatives to incarceration. A comprehensive approach to the collection and analysis of data on how well these programs are reducing incarceration costs, deterring crime, and improving public safety will help the Department to focus its resources and make strategic investments.

An essential building block to achieving performance-based management is having reliable data, an issue that has proven to be a challenge for the Department. Multiple OIG audits and reviews have identified problems with inaccurate or unreliable performance data. For example, in a 2014 review, the OIG found that the Department could not provide readily verifiable data related to its mortgage fraud efforts because of underreporting and misclassification of mortgage fraud cases in the Executive Office for U.S. Attorneys' case management system. The OIG also found there was no established methodology for obtaining and verifying the criminal mortgage fraud statistics announced during the Attorney General's October 2012 press conference regarding the Distressed Homeowner Initiative. According to an August 2013 FBI memorandum, the statistics presented at the press conference had reported approximately five times the actual number of criminal defendants charged as part of the initiative, and ten times the actual total estimated losses associated with Distressed Homeowners cases. Also, a 2014 OIG audit of the John R. Justice grant program found that the Bureau of Justice Assistance did not collect standardized, relevant baseline information on staffing rates for prosecutor and public defender positions, which resulted in limited data being available for a quantitative analysis of the impact of the grant program. In a 2012 review, the OIG found that the Executive Office for Immigration Review's performance reporting was flawed for both the immigration courts and the Board of Immigration Appeals. As a result, the Department could not accurately assess how well these bodies were processing immigration cases and appeals, or identify needed improvements.

Current and reliable data on performance measures is also critical in addressing resource allocation. Of growing importance in the current budget climate is the need to invest wisely in human capital, a fundamental prerequisite for achieving performance-based management. Between January 2011 and December 2013, the number of individuals employed by the Department declined by more than 4,000 due to sequestration and managed hiring efforts. Moreover, according to a January 2014 GAO report, by September 2017 approximately 28 percent of Department employees who were on board in September 2012 will be eligible to retire. The Department's FY 2015 budget request includes an increase of 580 positions over the FY 2014 enacted level. As the Department hires employees to fulfill its mission, it will need to rely on performance data to make strategic workforce planning and human capital decisions. The Department recently issued its human capital strategic plan for FYs 2015-2018 and plans to conduct quarterly data-driven reviews to measure its progress toward achieving the plan's goals.

In sum, effectively implementing performance-based management remains an ongoing challenge for the Department. Although the Department has taken actions to meet the requirements of the GPRA Modernization Act, it must continue to reexamine its performance measures. The use of reliable data will aid the Department in effectively measuring its programs, which in turn will enhance the Department's ability to achieve its strategic management objectives and allocation of resources.

5. Ensuring Effective and Efficient Oversight of Law Enforcement Programs

The Department's traditional law enforcement mission of enforcing and upholding federal law remains vitally important and occupies a central place in the Department's current strategic plan. As the nation's largest law enforcement agency, the Department possesses the unique responsibility of overseeing the coordination of its law enforcement practices while respecting civil rights. The OIG's recent work has identified several challenges facing the Department's law enforcement efforts.

A persistent challenge for the Department is to provide careful management and oversight of sensitive law enforcement programs. Such programs are not always subject to public scrutiny, heightening the importance of effective oversight. For example, our prior review on Operation Fast and Furious determined that the 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. We recommended that the Department coordinate among its law enforcement components on issues relating to significant law enforcement policies and procedures, case deconfliction mechanisms, and law enforcement initiatives. In this way, the Department can establish best practices and consistency among the investigative techniques used by its law enforcement components. The OIG is conducting a follow-up review to evaluate the progress and effectiveness of the measures the Department and the ATF have taken to implement the recommendations in our 2012 report that reviewed ATF's Operation Fast and Furious. Another key finding in our Fast and Furious report was that the ATF failed to exercise sufficient oversight of sensitive activities that posed a danger to the public or otherwise presented special risks. The ATF recognized this problem and established a Monitored Case Program to improve its oversight capabilities. The OIG is currently conducting a review to examine several ATF storefront operations that continued or began after the inception of the Monitored Case Program, and to evaluate the effectiveness of the Monitored Case Program as an oversight tool.

In addition, the OIG is reviewing the DEA's management of its confidential source program to evaluate its compliance with laws and regulations and oversight of payments to confidential sources. In particular, the OIG is determining if the DEA adhered to all requirements in the Attorney General's Guidelines regarding the use of confidential informants. This review will examine whether the Department reviews certain decisions relating to the registration and utilization of confidential sources. Concurrently, the OIG has been conducting an investigation of alleged payments for information by DEA personnel to an Amtrak employee. The OIG is also reviewing the Department's admission, handling, tracking, and monitoring of sex offenders admitted into the federal Witness Security (WITSEC) program and the Department's procedures for notifying states, local municipalities, and other law enforcement agencies regarding the relocation of the sex offenders in the WITSEC program.

Adding to the Department's oversight challenges is the need to integrate rapidly evolving technologies into law enforcement efforts while the rules governing those technologies remain in flux. The OIG is auditing the Department's use of or participation in law enforcement operations using unmanned aerial systems (UAS). Since the release of our September 2013 interim report, the Department has

convened a UAS policy review working group, but has not yet finalized action towards a Department-wide policy on the use of UAS. The Department should take appropriate steps to ensure the most efficient, effective, and appropriate use of this new law enforcement technology.

The Department also must balance its critical oversight of law enforcement programs with ensuring the civil rights of American citizens. For example, passenger interdiction is a sensitive activity that requires careful management. The OIG is examining interdiction activities involving DEA-initiated cold consent encounters and searches of travelers at transportation facilities. In this review, the OIG seeks to determine how DEA's policies and practices are currently being implemented and whether they can be improved to strengthen oversight and increase protection of civil rights.

At the international level, the Department has an expansive presence in foreign countries, including over 1,200 permanent positions in over 140 countries. Department personnel establish and maintain working relationships with other nations, provide training, assist with investigations, and transport fugitives back to the United States. The Department faces numerous cooperation and oversight challenges, particularly when helping to build foreign counterparts' law enforcement capacities to address the expansion of transnational crime. When foreign partners make a commitment to law enforcement reform, the Department can provide federal resources and expertise, including the International Criminal Investigative Training Assistance Program and the Office of Overseas Prosecutorial Development, to assist with investigative, prosecutorial, and correctional services. While the Department works with foreign partners to support national security and foreign policy objectives, including combatting illegal immigration and building national defense programs to fight terrorism abroad, it must also ensure that the coordination, management, and oversight of these efforts sufficiently address international issues and align with current U.S. government and Department concerns and missions.

Furthermore, careful and effective oversight of law enforcement activities and employee conduct abroad is essential given the potential impact on U.S. foreign interests. For example, as representatives of the U.S. government, off-duty misconduct by Department employees stationed abroad can present unique concerns, particularly for law enforcement employees with security clearances. Moreover, when off-duty misconduct occurs, the impact on the U.S. government's reputation and on its law enforcement efforts can be especially damaging. The OIG is currently reviewing policies, guidance, and training that govern the off-duty conduct of Department employees on official travel or assignment in foreign countries. In addition, the OIG and the Department of State (State) OIG are conducting a joint review of post-incident responses by the DEA and State to three 2012 drug interdiction missions in Honduras involving the use of deadly force. This review will address several issues, including the rules of engagement governing the use of deadly force and information provided to Congress and the public by the Department and State about the incidents.

Coordination among law enforcement entities is critical to ensuring effective and efficient law enforcement operations. In a recent review that examined the operations of the multi-agency Organized Crime Drug Enforcement Task Forces Fusion Center (OFC), we found that a strained working relationship between the

leadership of the OFC (the Director of which was a DEA employee during the OIG review) and the FBI created an uncooperative working environment that harmed the operations of the OFC. We also made several recommendations to improve the efficiency and effectiveness of OFC operations and usefulness of its analytic products, including that the Office of the Deputy Attorney General evaluate the structure of the OFC and the procedures for appointment of its management and staff to determine if modifications are appropriate to ensure efficient and cooperative operations.

Coordination is also a key tool for the Department in sharing the responsibility to patrol and manage more than 55 million acres of land with more than 500 federally recognized Native American tribes. In Indian Country, where there are high rates of violent crime, sexual assault, and substance abuse, federal law enforcement is both the first and likely only avenue of protection for victims of violent crimes. In particular, the impact and exposure to violent crime for Native American children is alarming, and it has been calculated that native youths are two-and-a-half times more likely to experience trauma compared to their non-native peers. The Department has requested $395.4 million to enhance and coordinate public safety initiatives in Indian Country. Additionally, the Department's Office of Justice Programs (OJP) awarded grants totaling over $263 million, through the Correctional Systems and Correctional Alternatives on Tribal Lands Program. The OIG is currently auditing this program to assess the OJP's management and oversight of the funding, as well as the OJP's cooperation and coordination with the Bureau of Indian Affairs to ensure efficient and effective correctional services in Indian Country.

As evidenced by the OIG's wide array of reviews relating to law enforcement issues, the Department continues to be challenged in its oversight role of the vast variety of complex and evolving law enforcement issues. It is crucial that the Department ensure proper oversight of its programs while acting consistent with the protection of civil rights for American citizens.

6. Upholding the Highest Standards of Integrity and Public Service

Charged with enforcing the nation's laws and defending its interests, the Department's senior officials and employees are expected to uphold the highest standards of integrity. Meeting this expectation is a key component in fulfilling the Department's crucial role in public service.

It is impossible for any organization as large and complex as the Department to maintain a perfect record of integrity, yet we have found that constant vigilance by the Department has produced positive results. For example, the FBI Laboratory (Lab) strengthened its latent fingerprint identifications by implementing major reforms, the USMS issued a promotional items policy to limit purchases of "swag," and the Civil Rights Division took steps to improve public confidence in the division's hiring practices have assisted in restoring public confidence in the Department.

Yet, the Department must ensure the fair administration of justice or public confidence may be lost. As evident from our July 2014 report describing irregularities in the FBI Lab, the OIG found serious deficiencies in the design, implementation, and overall management of the case review process conducted by a Department Task Force that responded to troubling findings about the FBI Lab in a 1997 OIG report. The deficiencies led to the Department's failure to ensure that capital cases were the Task Force's top priority and treated with urgency. For

example, three defendants were executed before their cases were identified and reviewed by the Task Force. Another significant deficiency arose from the Task Force's failure to review all cases involving an FBI Lab Examiner whose misconduct was identified in the OIG's 1997 report, and whose work was known by the Task Force as early as 1999 to be consistently problematic. Additionally, the OIG's July 2014 report regarding the DEA's detention of a suspect in San Diego found that the DEA's failure to ensure that the suspect was released from custody after deciding that he would not be charged resulted in his unjustified incarceration for 5 days, and in injuries requiring significant medical treatment.

The Department should also strive to maintain the highest standards of integrity and accuracy when reporting on its efforts to the public. In our 2014 Mortgage Fraud review, referenced above, we found that the Department did not prioritize mortgage fraud at a level commensurate with its public statements about its enforcement priorities and substantially overstated its mortgage fraud enforcement efforts by providing inaccurate statistics at its October 2012 press conference. Moreover, the Department became aware soon after the press conference that the statistics were seriously flawed, but did not inform the public of the errors until August 2013 and continued to cite them during the intervening 10 months. Providing the public with inaccurate information and failing to correct such misstatements in a timely manner erodes the public's confidence and trust in the Department.

The Department must continue to work to eliminate nepotism and favoritism in its hiring decisions and to abide by merit system principles. In 2012, the OIG issued a report on its investigation of improper hiring practices in the Department's Justice Management Division (JMD). We found that multiple JMD employees had violated applicable statutes and regulations in seeking employment for their relatives within JMD. In 2014, we determined that the recommendations we made in our report could be closed because of the steps JMD had taken to improve its hiring procedures. In September 2014, the Deputy Attorney General issued a memorandum directing all Department components to adopt hiring disclosure procedures similar to those adopted by JMD in response to the OIG report. In November 2014, the OIG found violations of the federal nepotism prohibition and other personnel rules arising from the hiring of four students who were relatives of the three most senior officials in the Executive Office of Immigration Review (EOIR). However, we also found that EOIR has taken steps to adopt hiring practices consistent with those adopted by JMD, which should help prevent nepotism and favoritism in future EOIR hiring. The OIG is nearing completion of an investigation of nepotism and favoritism in another DOJ component.

Whistleblowers play a crucial role in helping to ensure that the Department is upholding the highest standards of integrity and public service. For example, the OIG first learned about the DEA's unjustified detention of the suspect in San Diego, discussed above, when concerned individuals called the OIG's hotline regarding the matter. Yet, we continue to identify instances where Department employees have sought to retaliate against whistleblowers. One recent OIG investigation found that a former high-ranking ATF official made highly inappropriate and derogatory statements about the ATF agents who reported their concerns regarding Operation Fast and Furious. Another investigation found substantial evidence that one of these ATF agents was retaliated against by a former United States Attorney for his testimony before a Congressional committee. More recently, two FBI agents detailed to the OFC told us that they had been subjected to retaliation by the OFC Director

after they had raised concerns to the OIG about the OFC's operations. The OIG recently completed its review of these retaliation allegations and concluded that there were reasonable grounds to believe that actions were taken against the FBI employees in reprisal for making protected disclosures. The OIG continues to emphasize, through our OIG's Whistleblower Ombudsman Program, the vital importance of whistleblowers to ensuring the effective and efficient operations of the Department, as we seek to expand whistleblower training to all Department components. The Department's leaders must ensure that employees can come forward and report waste, fraud, abuse, and mismanagement without fear of retaliation, and that they know where and to whom they can report their concerns.

Robust oversight is critical to ensure that the Department upholds the highest standards of integrity. For any OIG to conduct effective oversight, it must have complete and timely access to all records in the agency's possession that the OIG deems relevant to its work. Prompt and complete access to information is a cornerstone of effective independent oversight by the OIG, a principle codified in the Inspector General Act. We expect that most OIG audits and reviews will be conducted with prompt and complete cooperation from Department components, yet there have been recent occasions when we have not obtained timely or complete access to certain records due to the Department's view that access was limited by other laws. Actions that limit, condition, or delay access to information have substantial consequences that may adversely affect our ability to provide efficient and thorough oversight of the Department.

The Department continues to face challenges regarding its handling of allegations of misconduct by Department attorneys. The Office of Professional Responsibility (OPR) has jurisdiction, by statute, to investigate allegations of misconduct against Department attorneys acting in their capacity as lawyers. The OIG has long questioned the carving out of this exclusive role for OPR as it is managed as a component of the Department, has no institutional independence, and lacks transparency in that it does not regularly release its reports and conclusions to the public. The independent, non-partisan Project on Government Oversight (POGO) issued a March 2014 report that was critical of OPR's longstanding lack of transparency and recommended empowering the OIG to investigate misconduct by Department attorneys. 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. Although a federal regulation, 28 C.F.R. 0.29e(a)(6), authorizes the OIG to request that the Deputy Attorney General assign to us a matter within the investigative jurisdiction of OPR, this procedure leaves the decision entirely to the Department leadership and, in any event, requiring the OIG to seek the Department's permission before undertaking an investigation compromises our independence. For these reasons, we continue to believe that Congress should eliminate this carve-out from the OIG's jurisdiction and support S.2127, bipartisan legislation that would amend the Inspector General Act to enable the OIG to investigate allegations of attorney misconduct.

The Department is expected to uphold the highest levels of integrity to maintain the public's trust. To meet this challenge, the Department must continue to encourage its employees to report what they reasonably believe to be evidence of wrongdoing, take steps to promptly address deficiencies, and ensure that oversight of its operations promotes the fair and impartial administration of justice.

7. Protecting Taxpayer Funds from Mismanagement and Misuse

Avoiding wasteful and ineffective spending is a fundamental responsibility of all federal agencies, and with a FY 2014 budget of $27.3 billion, the Department needs to ensure that it operates as efficiently and effectively as possible. In FY 2014, the OIG's reports, including those related to audits performed by independent auditors pursuant to the Single Audit Act, identified about $23.7 million in questioned costs and more than $1.2 million in taxpayer funds that could be put to better use. These figures are in addition to numerous recommendations for program improvements that are not quantified in dollars.

The Department must remain particularly vigilant when taxpayer funds are distributed outside of its direct control to third parties, such as grantees and contractors. Over the past decade there has been significant growth in the Department's contract spending. According to data from the government's USASpending.gov website, Department contract outlays almost doubled from $3.4 billion in FY 2003 to $7.3 billion in FY 2013. This growth in contract spending presents a challenge to the Department to ensure contracts are being awarded competitively, that the Department actively monitors contractor performance, and that funds are spent wisely and efficiently so that the Department gets full value for its expenditure of the taxpayers' money.

Nowhere is the growth trend in contracting more apparent than in the BOP. The BOP's FY 2015 budget requested $1.1 billion for contract prisons, representing 15 percent of its total budget. Additionally, as noted above, the proportion of federal prison inmates in contract facilities has risen from 2 percent in 1980 to 19.5 percent in 2013. Moreover, according to the Federal Procurement Data System, in FY 2013, 8 of the top 10 high-dollar Department contract obligations (funds set aside for payment) were for private prison contracts. Such cost information inevitably leads to the question: are private prisons more or less cost effective than public prisons? The OIG is currently examining how the BOP manages its private prison contracts. The OIG is also auditing one of the largest BOP private prison contracts, which was awarded to a detention center in Texas, to assess the BOP's and contractor's compliance with contract terms and conditions in the areas of billings and payments, staffing requirements, and contract oversight and monitoring.

In part due to the sheer volume of money and the large number of recipients involved, grant funds present a significant risk for mismanagement and misuse. According to USASpending.gov, from FY 2009 through FY 2013 the Department awarded approximately $17 billion in grants to thousands of governmental and non-governmental recipients. For example, an OIG audit questioned nearly all of the more than $23 million in grant funds awarded by the Department to Big Brothers Big Sisters of America (BBBSA) due to the mismanagement of the grant funds. The audit also resulted in the OJP freezing disbursement of Department grant funds to BBBSA at that time. However, four months after OJP's action, BBBSA received $5 million in grant funds from the Department of Labor. Further, we understand that OJP has recently approved a partial release of funds to BBBSA under BBBSA's 2012 grant based upon OJP's approval of a 90-day budget of BBBSA's anticipated costs, and that BBBSA may request drawdowns on a reimbursement basis as expenses are incurred. Protecting taxpayer funds from mismanagement and misuse is critical, and the Department must ensure that when such actions are taken with respect to a grant recipient, it

should communicate with other federal granting agencies so that they are aware of the Department of Justice actions.

Further, the OIG's recent reports have identified several opportunities for improved efficiency in how the Department spends its own funds. For example, as described above, our June 2014 audit examined the BOP's purchase and usage of x-ray machines, and found significant concerns in the effectiveness and usage of the x-ray machines. The OIG found that the machines were not effective for screening certain commodities commonly received by BOP institution warehouses. In addition, significant delays between the delivery and installation of some x-ray machines resulted in over $182,000 in expended funds for which no benefit had been realized.

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 2013, the Department reported recoveries of $3.8 billion in False Claims Act cases primarily comprised of $2.6 billion attributable to health care fraud civil recoveries and $890 million attributable to procurement fraud. The OIG's Fraud Detection Office (FDO) has opened grant fraud cases on issues including consultant payments, conflicts of interest, and embezzlement, and has provided fraud awareness training to OJP. In 2014, the FDO conducted 28 briefings focused on grant fraud indicators and common schemes, which reached approximately 2,500 participants.

The Department must also use all appropriate tools available to recover money owed to it, enforce the collection of debts owed to crime victims and the federal government, and ensure that the amounts recovered from civil debt collection activities are properly credited to the Department and spent wisely. In FY 2013, the USAOs collected $9 billion in criminal and civil debts. However, at the end of FY 2013, an additional $25.3 billion was owed to the United States, including $20.8 billion in criminal fines and restitution and $4.5 billion in civil debts. The USAOs' efforts to collect criminal and civil debts are the subject of an ongoing OIG review.

The Department must also ensure the proper stewardship of its Assets Forfeiture Fund, which has seen a significant increase from $2.9 billion in FY 2011 to $5 billion as of FY 2013. A portion of these funds constitutes the Department's Equitable Sharing Program, which distributes a share of forfeited property and proceeds to state and local law enforcement agencies that participate in a federal forfeiture. The equitable sharing payments distributed to state and local law enforcement agencies increased from nearly $440 million in FY 2011 to nearly $710 million in FY 2013. While this program offers the Department and its state and local partners a collaborative opportunity in law enforcement, if not carefully managed, the program also creates an opportunity for abuse. For example, in the past two fiscal years, OIG audits of equitable sharing payments identified over $2 million in questioned costs. The Department must maintain careful oversight of the equitable sharing payments it distributes to ensure that state and local agencies spend these funds appropriately. The Department's oversight must also ensure that state and local agencies obtain forfeited property and proceeds in an appropriate manner.

The OIG's recent oversight work has demonstrated the continued challenges the Department faces in ensuring that taxpayer funds are protected from fraud, mismanagement, and misuse. It is essential that the Department continue to manage its resources wisely and maximize the effectiveness of its programs even as the Department's current budget environment improves.