

Section III

Management Section (Unaudited)

Overview

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

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

This page intentionally left blank.



Top Management and Performance Challenges Facing the Department of Justice

November 10, 2015

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 2015 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 eight challenges that we believe represent the most pressing concerns for the Department:

- Achieving Balance and Containing Costs in a Significantly Overcrowded Federal Prison System
- Enhancing Cybersecurity in an Era of Increasing Threats
- Building Trust and Improving Police-Community Relationships
- Safeguarding National Security Consistent with Civil Rights and Liberties
- Ensuring Effective Oversight of Law Enforcement Programs
- Promoting Public Confidence by Ensuring Ethical Conduct throughout the Department
- Effectively Implementing Performance-Based Management
- Protecting Taxpayer Funds from Mismanagement and Misuse

We believe addressing the federal prison crisis and cybersecurity threats are particular challenges that will continue to occupy much of the Department's attention and require vigilance in the foreseeable future. In addition, we have identified a new challenge, *Building Trust and Improving Police-Community Relationships*, as an emerging issue where the Department must demonstrate leadership, provide support, and exercise oversight in its capacity as the federal agency charged with enforcing the law. Meeting all of these challenges will require the Department to develop innovative solutions and exercise careful oversight to ensure the effectiveness of its operations.

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

Attachment.

This page intentionally left blank.

**TOP MANAGEMENT AND PERFORMANCE CHALLENGES FACING THE
DEPARTMENT OF JUSTICE**
Office of the Inspector General



Source: BOP website

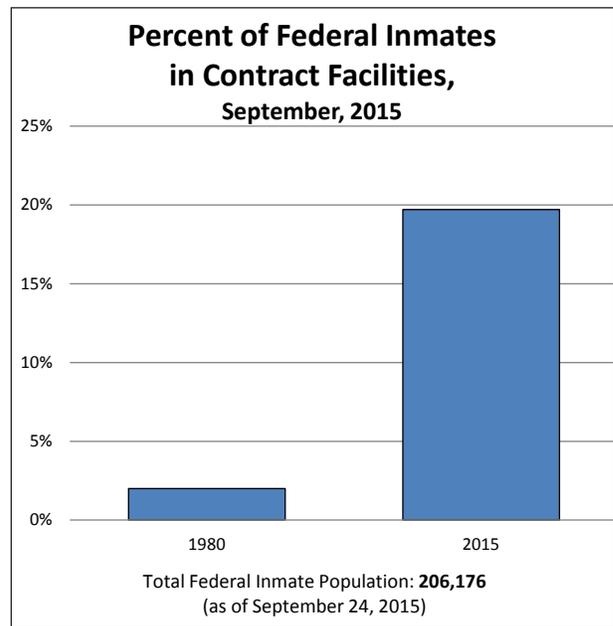
1. Achieving Balance and Containing Costs in a Significantly Overcrowded Federal Prison System

Though the number of federal inmates has declined for a second year in a row, the Department of Justice (Department or DOJ) continues to face a crisis in the federal prison system. Continued high rates of overcrowding both negatively impact the safety and security of staff and inmates and drive costs upward. While the Federal Bureau of Prisons (BOP) must ensure a secure environment and meet the medical and programming needs of its inmates, it must also balance these activities with regard to cost. However, meeting this challenge is complicated by the fact that the BOP exercises little control over the number of inmates it must house. The Department must therefore pursue a comprehensive approach to managing its federal inmate population, in order to find an appropriate balance that addresses the safety of the public, staff, and inmates in the federal prison system while holding costs to manageable levels.

Improving Prison Safety and Security

Ensuring the safety and security of the BOP staff, inmates, and the public is critical. The BOP continues to face dangerous levels of overcrowding at its institutions, which poses threats to both staff and inmates. While the BOP has experienced some reduction in the inmate population in the past 2 years, the fiscal year (FY) 2014 Agency Financial [Report](#) has once again identified prison overcrowding as a programmatic material weakness, as it has done in every such report since FY 2006. Moreover, although overall overcrowding decreased from 33 percent in June 2014 to 26 percent in August 2015, overcrowding at high security institutions has actually increased from 42 percent to 51 percent. This presents a particularly significant concern because more than 90 percent of high security inmates have a history of violence, making confinement in such conditions especially problematic. In addition, the BOP has acknowledged that its inmate-to-correctional officer ratio remains undesirably high, and indicated that at times it has had to rely on non-custody staff to assist in covering security posts.

The difficulties in ensuring safe and secure incarceration of federal inmates apply not only to BOP-managed institutions, but also to contract facilities. As of September 2015, nearly 20 percent of federal inmates were housed in contract facilities, an increase from 2 percent of the inmate population in 1980. This total includes approximately 24,000 inmates housed in BOP's 13 privately-managed contract prisons. Although contract prisons may in some cases help to alleviate overcrowding of BOP facilities, contract prisons also can present safety and security risks for staff and inmates. For example, a riot perpetrated by approximately 2,000 inmates at the privately-managed Willacy Correctional Center earlier this year resulted in staff injuries and extensive property damage. Soon afterwards, the BOP cancelled the Willacy contract and transferred its inmates to other facilities. There have been riots at other BOP contract prisons in recent years, including one in 2009 and another in 2012 that resulted in the death of a correctional officer, severe injuries to both staff and inmates, and extensive property damage. The Office of the Inspector General (OIG) is completing a review examining how the BOP monitors its contract prisons and whether contract performance meets inmate safety and security requirements. The OIG will also evaluate how contract prisons and similar BOP institutions compare in an analysis of inmate safety and security data. The BOP and the Department need to ensure that contract facilities provide a safe and secure environment for inmates, staff, and the public, and that they do so in a cost effective manner.



Source: BOP

The use of segregated housing in both contract facilities and BOP institutions raises significant challenges. As mentioned in last year's management challenges [report](#), the BOP underwent an independent assessment of its use of restrictive housing, including both single-inmate and multiple-inmate cells. The assessment, completed in December 2014, resulted in over 20 findings, including concerns regarding the use of restrictive housing for inmates with severe mental illnesses. The report also concluded that the BOP needed to improve its mental health diagnoses, offer more effective treatment, and provide sufficient psychiatric staffing. While the BOP uses restrictive housing primarily to confine dangerous inmates, it must weigh the use of this option, particularly for those with mental illnesses, given the potential negative psychological effects attendant with such types of confinement. The 2014 report recommended moving seriously mentally ill inmates into alternative units to reduce the number of inmates placed in restrictive housing. The OIG is currently conducting an evaluation of the screening, monitoring, and treatment of mentally ill inmates in BOP's restrictive housing units, evaluating costs and mental illness trends across several restrictive housing units. This review should help inform the BOP's efforts in this area, which implicate the difficult task of ensuring the safety and security of the facility while not undermining the mental health and rights of its inmates.

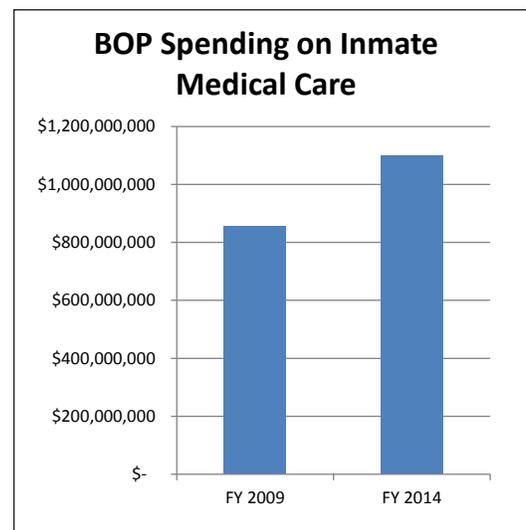
Preventing the introduction of contraband is another challenge to ensuring safety and security in BOP facilities. Cell phones are a particularly dangerous contraband item in a prison because inmates can use the devices to carry out criminal activities – such as coordinating additional contraband smuggling; threatening and intimidating witnesses, victims, and public officials; and orchestrating escape attempts. To help prevent the introduction of contraband, the BOP has introduced various technologies, including piloting in September 2014 the use of Millimeter Wave Scanners for contraband detection at six institutions. Also, in July 2013, over 10 years after a January 2003 OIG [report](#) recommended that the BOP implement a staff entrance and search policy, the BOP implemented new staff entrance and search procedures that authorized

random pat searches of staff and their belongings. However, as a result of a recent Federal Labor Relations Authority ruling that concluded, in substance, that staff search policies were not negotiated properly, the BOP rescinded the 2013 search policy and reinstated the prior procedures. The OIG continues to investigate and present for prosecution an ongoing stream of cases involving the introduction of contraband into BOP facilities, and we are engaged in an ongoing review of the BOP's contraband interdiction efforts, to include an evaluation of staff searches as well as physical security measures, including random pat searches and TSA-style body scanners. The results of these cases and our review should be instructive for the BOP as it continues to battle against new and innovative means of introducing dangerous contraband that threaten the safety and security of inmates and staff.

Containing the Cost of the Federal Prison System

While the Department faces the challenge of maintaining safety and security in the federal prison system, it must also look for ways to contain ballooning costs. As the costs to operate and maintain the federal prison system continue to grow, less funding will be available for the Department's other critical law enforcement and national security missions, making effective management of the federal prison system a significant challenge the Department cannot ignore. The BOP currently has the largest budget of any Department component other than the Federal Bureau of Investigation (FBI), accounting for more than 25 percent of the Department's discretionary budget in FY 2015, and employing 34 percent of the Department's staff. The BOP's enacted budget was nearly \$7 billion in FY 2015, an 11-percent increase since FY 2009, despite a decline in the federal prison population from 214,149 in FY 2014 to 206,176 in FY 2015 – its lowest level in 6 years. Further, the BOP has requested an additional 6-percent increase for next year, despite projecting that its population will decrease by an additional 12,000 inmates.

The Department must isolate the chief drivers of these uncontrolled costs and consider innovative solutions that might help to contain them. As mentioned in last year's management challenges report, inmate medical costs are a major factor in BOP's overall rising costs and thus an area that must be monitored closely. In FY 2014, the BOP spent \$1.1 billion on inmate medical care, an increase of almost 30 percent in 5 years. One factor that has significantly contributed to the increase in medical costs is the sustained growth of an aging inmate population – a 2015 OIG [report](#) found that the oldest BOP inmates cost an average of \$30,609 each or 65 percent more than the youngest ones. As a result, we recommended revising the requirements that limit the availability of compassionate release for aging inmates. One consequence of the increase in the aging inmate population is BOP's increased need for inpatient treatment beds, which has grown by 67 percent since 2003. In addition, the BOP is spending significantly more to meet the needs of aging inmates with serious diseases.



Source: BOP

The Department must also assess the cost-effectiveness of the BOP's increasing reliance upon contract services to provide more facility space and supplement medical care. The BOP contracts with 13 prisons owned by either county governments or private prison companies to confine inmates who are primarily low security, foreign nationals with less than 90 months remaining in their sentences. In the past 5 years, spending for contract prisons increased by more than 30 percent, to \$639 million in FY 2014. The BOP needs to remain vigilant in assessing the cost effectiveness of procuring contract services, particularly in light of reforms to reduce its overall inmate population. As the OIG's 2015 [audit](#) of the Reeves County,

Texas contract prison showed, the Department must conduct careful oversight of these contracts. In auditing that contract alone, we found nearly \$3 million in questioned costs. Our work has also found that the BOP struggles to meet the medical needs of its inmates with its own staff and must use contracts to supplement the medical care it provides. According to BOP data, spending for inmate medical services provided by contract providers increased 27 percent from \$258 million in FY 2010 to \$327 million in FY 2014. The OIG is currently examining factors that contribute to BOP's medical staffing challenges as well as the financial impact of using contract medical care. We believe that this analysis should help the BOP identify ways to address this pressing issue.

Properly Evaluating Other Department Programs and Policies Can Better Address the Prison Crisis

The challenges to the federal prison system cannot be corrected by the BOP alone, as it has only limited control over the number of inmates it is charged with safely housing. Instead, multiple Department-level efforts must come together if there is any hope of seriously addressing these safety, security, and cost concerns. To address these and other challenges, the Department launched the Smart on Crime [initiative](#) in August 2013, with the goal of reforming the federal criminal justice system by curbing reliance on incarceration for less dangerous offenders. The initiative proposes taking a comprehensive approach to the criminal justice process by focusing on five key goals: (1) prioritize prosecutions to focus on the most serious cases; (2) reform sentencing to eliminate unfair disparities and reduce overburdened prisons; (3) pursue alternatives to incarceration for low-level, non-violent crimes; (4) improve reentry to curb repeat offenses and re-victimization; and (5) provide “surge” resources to aid violence prevention and protect the most vulnerable populations. Proposed reforms include requiring districts to modify their guidelines for when federal prosecutions should be brought, limiting the use of mandatory minimums and enhancements for repeat offenders for low-level, non-violent drug defendants, and enhancing prevention and reentry efforts at each U.S. Attorney's office.

The Smart on Crime initiative also aims to explore cost-effective reforms to the federal prison system that will allow law enforcement to redirect scarce federal resources toward violence prevention. For example, a 2014 Government Accountability Office (GAO) [report](#) estimated that 370,985 beds and \$4.1 billion could be saved in the next several years through retroactively reducing prison sentences for inmates currently incarcerated for certain drug offenses. The GAO found that other options, such as not bringing charges that carry mandatory minimum sentences in cases involving low-level, non-violent drug offenders, would have less of an impact, but still could provide relief for the federal prison system as well as redirect resources to crime prevention.

As an outgrowth of the Smart on Crime initiative, the Department established its new clemency [initiative](#) in April 2014. Under this initiative, the Department indicated that it will prioritize clemency applications for non-violent, low-level inmates who petition to have their sentences commuted or reduced by the President. In addition, as part of Smart on Crime, the Department has announced its intention to expand the use of pre-trial diversion and drug court programs to provide alternatives to incarceration and reduce recidivism. These two alternatives enable prosecutors, judges, and probation officers to divert certain offenders from traditional criminal justice proceedings into programs designed to address the underlying causes for criminal behavior or otherwise provide appropriate sanctions and remedies without the need in many cases for incarceration or even criminal convictions. The OIG is currently evaluating the use of these programs within the various U.S. Attorneys' Offices.

We have found that the Department could better utilize other programs and policies related to the goals of the Smart on Crime initiative. In August 2013, as part of the Smart on Crime efforts, the BOP expanded its Compassionate Release Program. This change allowed inmates age 65 and older to request a reduction in

sentence if they meet certain criteria. However, our subsequent [report](#) on the BOP's aging inmate population found that during the first year after the new BOP policy was implemented, only 2 of the 348 inmates who applied were released under the new provisions. The OIG found that the Department imposed several restrictive requirements, including a rule that inmates requesting a non-medical compassionate release must have already served 10 years and 75 percent of their sentences to be eligible for compassionate release. By excluding inmates with sentences of less than 10 years, this change significantly reduced the number of inmates who could apply and, as a consequence, excluded many who committed lesser, non-violent offenses. Similarly, in an August 2015 follow-up [report](#) on the Department's international treaty transfer program, the OIG found that the number of inmates transferred under the program had actually decreased, despite a substantial increase in both awareness of the program and the number of inmates applying for such transfers. The OIG's follow-up report recommended that Department leadership boost the effectiveness of this program by actively engaging with treaty transfer partners, including the Department of State and foreign government representatives.

Among the more difficult challenges that the Department faces is adequately measuring whether these various initiatives will ultimately meet its goal of reducing the prison population and containing costs. In many reports we have found that the Department needs better recordkeeping to be able to evaluate and direct its efforts. This was confirmed in a 2015 GAO [report](#), which recommended that the Department modify its 16 Smart on Crime indicators to better track whether the program was having much success. In fact, the last BOP study on the overall recidivism rate for federal inmates occurred more than 20 years ago, which is concerning given the BOP spends hundreds of millions of dollars annually on reentry programs and residential reentry centers to improve rehabilitation efforts. As we describe more fully [below](#), the Department must develop the capability to accurately assess its initiatives and programs in order to properly measure their outcomes and efficacy, and that is particularly true given the limited resources available to conduct law enforcement and incarceration efforts within the Department.

In sum, a multi-faceted approach is necessary to address the persistent crisis in the federal prison system. The Department has taken several steps by pursuing programs and policies including its Smart on Crime initiative. Yet, the Department needs to collect the correct information to continuously evaluate whether these initiatives are reaching their goals, and put in place policies and practices designed to achieve them. The BOP must also continue to work collaboratively with other Department components to develop better methods to fully utilize its own programs, prevent the introduction of contraband, provide effective management of contract services, and address staffing and other challenges to the safety and security of its facilities.

2. Enhancing Cybersecurity in an Era of Increasing Threats



Source: FBI website

The Department, working closely with its private sector, law enforcement, and global partners, must be persistent and innovative in defending the nation's cyber resources from intrusions and attacks. In September 2015, Director of National Intelligence James Clapper testified that cyber threats pose one of the gravest national security risks to the United States. Further, a September 2015 GAO [report](#) concluded that federal agencies' information and systems remain at a high risk of unauthorized access, use, disclosure, modification, and disruption, while also noting an increasing number of cyber incidents and breaches of personal information at federal agencies. As recent events have shown, increasingly sophisticated attacks can result in significant releases of information and potential damage to national security. The breaches of Office of Personnel Management (OPM) data compromised the personal

information of more than 22 million people, and resulted in the disclosure of fingerprints and other highly sensitive data from background investigations of more than 5.6 million current, former, and prospective federal employees and contractors. That, combined with reported cyberattacks on other government agencies, clearly demonstrates that the federal government is vulnerable. The danger to private industry and American citizens is equally clear and present: private and public organizations as well as individual citizens continue to be victimized by cyberattacks. For example, earlier this year, a publicly reported cyberattack on health insurer Anthem Inc., exposed private data, including names and Social Security numbers, of nearly 80 million people. Other reported attacks on Target, Bank of America, and Sony, among others, are all too regular reminders of the critical need to better shield our nation's Information Technology resources.

Among the greatest challenges the Department faces in this area is that malicious actors are increasingly relying on encryption and other technological advances to remain elusive and thwart the government's efforts to isolate and mitigate cyber threats. FBI Director James Comey recently warned in testimony before the Senate Judiciary Committee that advances in encryption technology are allowing our adversaries to "go dark." The growing use of single-key encryption on smartphones and other devices restricts access and prevents communications providers from providing law enforcement with stored data, even if they obtain a court order. As it looks for ways to combat cybercrime and intrusions despite encryption technologies, the Department needs to find ways to assure citizens it will not violate their privacy rights – underscoring the inherent tension between cybersecurity, civil liberties, and national security. While strong encryption protects the right of Americans to communicate in private, free of government surveillance, allowing device users sole control over their data greatly limits law enforcement's ability to find and retrieve significant evidence that may reside on a smartphone, a tablet, or a laptop. This, in turn, has the potential to leave crime and national security threats undetected. The government must work with private industry to shape an encryption policy that strives to ensure that privacy and security can co-exist.



Source: DOJ OIG

As it devotes increased attention, resources, and personnel to its cybersecurity efforts, the Department needs to maximize their impact by developing and implementing a cohesive strategy to tackle this problem. In its FY 2016 budget, the Department requested an additional \$26.8 million to confront computer intrusions and cybercrimes and protect the Department's information networks from both internal and external threats. In May 2015, Assistant Attorney General Leslie Caldwell announced the creation of a new Cybersecurity Unit within the Criminal Division's Computer Crime and Intellectual Property Section. This unit is charged with assisting other government agencies and the private sector to develop and implement their cybersecurity plans consistent with federal law. This is in addition to the National Cyber Investigative Joint Task Force, run by the FBI under a presidential directive that makes the Department the focal point for coordinating, integrating, and sharing information on cyber threat investigations across 19 U.S. agencies and foreign partners. In October 2012, the FBI also launched its Next Generation Cyber Initiative (NextGen) and has requested nearly \$500 million for NextGen and its growing capabilities for the upcoming fiscal year. The goals of this initiative include improving cyber skills for agency personnel and strengthening public and private partnerships. The initiative has narrowed the focus of the FBI's Cyber Division to work solely on cyber intrusions that pose the greatest threat to national security and on being proactive in preventing future attacks.

But even as it works to expand the ranks of its cybersecurity team, the Department continues to face challenges recruiting and retaining highly-qualified candidates to do this work, as detailed in our July 2015 [audit](#) of NextGen. We found that the FBI failed to hire 52 of the 134 computer scientists that it was authorized to hire, and that 5 of the 56 field offices did not have a computer scientist assigned to that office's

Cyber Task Force. Among other hiring challenges the audit identified were that the FBI's background investigations are more onerous than those used by many private sector employers, and it was difficult to retain top talent because private sector entities often pay higher salaries. Addressing these systemic challenges will be difficult, but it will be essential if the FBI and the Department are to play the leading role in combating this threat.

Building closer relationships with the private sector, state and local law enforcement, and global partners is another way the Department can work toward its cybersecurity goals. Despite the Department's emphasis in its FY 2014-2018 Strategic [Plan](#) on establishing successful relationships with other law enforcement agencies and developing strong private-public partnerships, it continues to face challenges partnering and sharing information about cyber matters with private sector entities, in part because of privacy concerns and a general distrust of government. Our July 2015 NextGen audit found that few state and local law enforcement agencies are motivated to join their local Cyber Task Force for a variety of reasons that must be addressed by the FBI in order to foster greater participation. The audit also found that although the FBI is working to develop strategies to enhance outreach to private sector entities, it continues to face challenges partnering and sharing information with these entities. The OIG is currently reviewing the FBI's strategy to mitigate cyber threats through an approach for identifying the perpetrators and their tradecraft, intent, capabilities, and affiliation. Those findings should help to further inform the Department's efforts in this critical area.

Given that those posing cyber threats know no boundaries, the Department has recognized the importance of working closely with other countries to boost cybersecurity. In September 2015, Attorney General Loretta Lynch announced that combating cybercrime was one of her top priorities and pledged that the Department was prepared to play a global leadership role in this effort. In remarks at Europol, in the Hague, the Attorney General highlighted Department efforts to improve global cooperation by (a) establishing permanent Cyber Assistant Legal Attaché positions in London, Ottawa, and Canberra, and adding five new temporary positions; (b) hiring 38 additional attorneys and 26 professional staff to the Office of International Affairs Mutual Legal Assistance Treaty Modernization project, with the goal of facilitating the transfer of information regarding international cyber issues; and (c) temporarily assigning a U.S. prosecutor to sit at Eurojust, the European Union's Judicial Cooperation Unit, and work with Europol's European Cybercrime Centre. The Attorney General also announced that the United States and the European Union had initiated the "Umbrella" Data Privacy and Protection Agreement, designed to enhance the ability of law enforcement and prosecutorial agencies on both sides of the Atlantic to combat crime and terrorism while protecting personal privacy. These are positive steps, but the Department must continue to push forward to develop and expand effective partnerships with private entities and state, local, and foreign governments, as they are all critically necessary partners in the Department's cybersecurity efforts.

While looking outward, the Department cannot lose sight of the critical need to make sure its own cyber defenses are robust. Following the OPM breach, the Office of Management and Budget (OMB) directed agencies to patch critical vulnerabilities, review and tightly limit the number of privileged users with access to authorized systems, and dramatically accelerate the use of strong authentication, especially for such privileged users. Following OMB's directive, the White House reported that federal civilian agencies increased their use of strong authentication (such as smartcards) for privileged and unprivileged users from 42 percent to 72 percent. The Justice Department, however, had among the worst overall compliance records for the percentage of employees using smartcards during the third quarter of FY 2015 – though it has since made significant improvements, increasing to 64 percent of privileged and unprivileged users in compliance by the fourth quarter. Given both the very sensitive nature of the information that it controls, and its role at the forefront of the effort to combat cyber threats, the Department must continue to make progress to be a leader in these critical areas.

The Department must also ensure that recommendations to address the security and operations of its systems are promptly implemented. Pursuant to the Federal Information Security Modernization Act of 2002 (FISMA), each Inspector General performs an annual independent evaluation of the agency’s information security programs and practices. For FY 2014, the OIG provided 56 recommendations on five Department components’ information security programs which included one classified, and five unclassified systems. For FY 2015, the OIG also reviewed the security programs of five Department components, which included two classified systems, and four sensitive but unclassified systems. We plan to complete reports evaluating each of these systems as well as reports on each Department component’s information security program. Meanwhile, OMB has worked with the Chief Information Officers Council and the Council of the Inspectors General on Integrity and Efficiency to improve the reporting process and clarify FISMA reporting guidance for the inspector general community. We support the FISMA reform effort and believe it will help us provide more meaningful guidance to the Department on how it can be better prepared to prevent intrusions.

In an era of ever-increasing cyber threats, the Department will be challenged to sustain a focused, well-coordinated, and robust 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 lead the effort to combat cybercrime, identify and investigate perpetrators, and engage the private sector and its state, local, and global partners in this crucial effort.

3. Building Trust and Improving Police-Community Relationships



Source: OJP website

Among the most pressing challenges facing the Department is determining how it can most effectively assist in the vital task of mending the apparent growing divide between some of the nation’s communities and their police departments. The recent riots in Ferguson and Baltimore following the deaths of unarmed African-Americans during encounters with police – as well as several attacks resulting in the deaths of law enforcement officers in Houston and Brooklyn – highlight the tension and the potential erosion of trust between law enforcement officers and the people they serve in certain communities across the country. This tension and a resulting lack of trust has the potential to negatively impact the ability of law enforcement to function effectively, thereby affecting the safety of those communities, and possibly trigger other undesirable collateral consequences, including the loss of police morale that could further endanger public safety. As Attorney General Lynch recognized in remarks earlier this year, the country has seen “too frequently how relationships between communities and law enforcement can grow strained; how trust can be broken or lost; and how simmering tensions can erupt into unrest.” In order to provide leadership fighting crime, the Department must be able to rely on strong partnerships with state and local police departments. Only then can it gather street-level intelligence and benefit from the assistance of those officers closest to emerging threats. But if communities lose trust and confidence in their local police, or the police lose trust and confidence in local leaders, that will inevitably impact the ability of federal agents and prosecutors to join with local law enforcement to protect the citizenry. Further, if police experience lower morale due to a lack of support – perceived or otherwise – and deteriorating relationships with citizens in their communities, they may fear retribution or otherwise be less likely to aggressively fight crime. Recognizing this, Attorney General Lynch toured the nation earlier this year stressing that “restoring trust where it has eroded,” while fostering relationships between police and the communities they serve, is one of her top priorities as Attorney General. The Attorney General also has emphasized the critical role police officers play in ensuring public safety and stressed they merit the Department’s full support.

As the federal agency charged with enforcing the law, the Department can play a leadership role through cooperative law enforcement operations, grant funding of state and local efforts, knowledge and information sharing, and framing national discourse – not only with its own federal law enforcement components, the FBI, the Drug Enforcement Administration (DEA), the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and the U.S. Marshals Service (USMS), but also with state and local police. These partnerships will, in turn, help the Department be a more effective leader in protecting Americans from both domestic and international threats, thereby creating and maintaining safer communities across the country.

The Department’s task then is to determine how best to assist in solving a problem that is largely local in nature, when it has limited resources to share, limited jurisdiction upon which to act, and limited control over most aspects of crime fighting. We believe there are at least four areas where the Department can play a critical role: (a) providing leadership in improving the national dialogue between law enforcement and their communities; (b) offering and coordinating federal grants and guidance to local police departments to fund equipment, training, and reforms; (c) monitoring and assisting with the reform of police departments that are found to have engaged in a pattern or practice of unlawful misconduct, to include violating their citizens’ civil rights; and (d) investigating and prosecuting law enforcement officers, whether local, state, or federal, who violate federal civil rights laws.



Source: DOJ OIG

In its leadership role, the Department must find ways to use the tools it has to help guide and oversee changes needed at the community level. Shortly after the events and protests in Ferguson, the Department launched a national initiative to build trust between law enforcement and local communities. Through a 3-year \$4.75 million grant, the National Initiative for Building Community Trust and Justice, launched in September 2014, the Department designed “a new approach to training, policy development, and research geared toward advancing procedural justice, promoting racial reconciliation, and eliminating implicit bias.” The Attorney General has pointed out that an increased

effort in leadership and police-community partnerships led to a collaboration that has “transformed” certain cities. Additionally, the President signed Executive Order 13684 to establish the Task Force on 21st Century Policing to focus on improving policing practices. The task force recommended further research and suggested action items for law enforcement agencies, stakeholders, and the Department. Among its recommendations were that law enforcement agencies establish a culture of transparency and public trust by creating a more diverse workforce and making all department policies available to the public. These initiatives suggest a path the Department can follow to lead a national dialogue to develop and promote proactive solutions in this area.

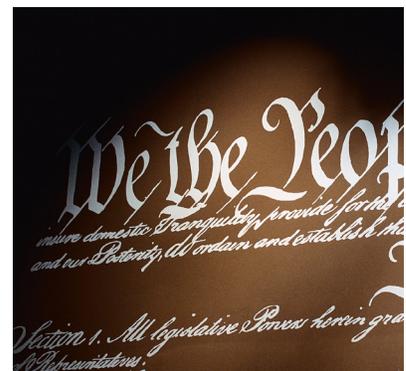
Another of the Department’s challenges is to use available resources to foster partnerships with state and local law enforcement agencies in order to support law enforcement and oversee improvement at the community level. DOJ components such as the Office of Justice Programs (OJP) and the Office of Community Oriented Policing Services (COPS) provide federal leadership and coordination in developing the nation’s capacity to prevent and control crime, administer justice, and advance public safety through community policing. These grant-making components can direct funding for training, equipment, and support to law enforcement entities across the country in furtherance of Department goals. The Department recently announced grant funding for its Smart Policing Initiative, with the goal of helping local law enforcement agencies reduce crime and earn the confidence of the citizens they serve. In September 2014 COPS also announced \$124 million in awards to fund 950 community policing officers at 215 law enforcement agencies across the country. COPS subsequently released a resource guide for police

agencies highlighting training, leadership, and initiatives available for local communities. In addition, in May 2015, the Department announced a \$20 million Body-Worn Camera Pilot program administered by OJP and designed to fund such programs in 73 local and tribal agencies across the country. The program's goals are to improve safety, reduce crime, and build community trust through the purchase of body-worn cameras, training and technical support to the recipient agencies, and identification of best practices.

Along these lines, to help evaluate what steps the Department can take to help reduce violence in local communities, the OIG has begun a review of the Department's violent crime initiatives. This review will evaluate the Department's strategic planning and accountability measures in combating violent crime, including coordination across Department prosecution, law enforcement, and grant-making components.

But as the Department wrestles with where and how it should invest to achieve the greatest impact with grants to local police departments, a major impediment is that it lacks complete and accurate data on issues driving the circumstances facing local law enforcement. In February 2015, FBI Director Comey stated that "the first step to understanding what is really going on in our communities and in our country is to gather more and better data related to those we arrest, those we confront for breaking the law and jeopardizing public safety, and those who confront us." Currently, complete figures on the number of "justifiable homicides" are unavailable because law enforcement agencies only voluntarily report this data. The FBI cannot completely track data on the number of incidents in which force is used by or against police officers. Without complete and accurate data, the Department and the American people do not have a complete picture of the nature of the problem, which undermines the potential effectiveness of any steps developed to address it. The Department has taken some early steps to help address this issue. In October 2015, the Attorney General announced that the FBI and the Bureau of Justice Statistics, in collaboration with major policing organizations, are working to expand and standardize relevant data collection. Going forward, the Department must improve the collection and analysis of data from local law enforcement agencies to determine the true nature of violent crime, "use of force," and officer-involved shootings.

In addition to providing supportive resources to police departments, the Department, through its Civil Rights Division (CRT), plays a critical role in ensuring that police departments use their powers consistent with the Constitution. CRT has investigated law enforcement agencies nationwide to address allegations of excessive force; unlawful stops, searches, or arrests; and discriminatory policing. Through these "pattern and practice" investigations, CRT endeavors to create models for effective and constitutional policing nationwide. The reforms sought by CRT at the departments it investigates can provide significant, systemic relief; increase community confidence in law enforcement; and improve officer and agency accountability. For example, after a CRT investigation showed that officers regularly used excessive force against Latinos in East Haven, Connecticut, city officials took steps to improve police-community relations. Among the reforms they adopted were requiring all officers to wear body cameras, holding regular community meetings, having school-based officers check on children, and creating a citizens' police academy. The Attorney General singled out the city's efforts as a model for improving relations between police and the community.



Source: DOJ

In the past 6 years, according to the Department, CRT has opened "pattern and practice" investigations in 22 police departments across the country. CRT and U.S. Attorneys' Offices also criminally prosecute law enforcement officers across the country for violating individuals' civil rights. Ultimately, civil rights investigations of police departments and criminal prosecutions of police officers are only two tools to help build trust in local law enforcement, and the Department needs to evaluate what methods will be most effective in helping the nation address the larger issues at stake.

The Department must work through these critical issues to determine how to best use its limited but substantial resources to help foster partnerships, support law enforcement efforts across the country, and ensure confidence in community-police relations. Effective policing at the state and local level contributes significantly to the success of law enforcement efforts at the federal level. By dedicating resources for funding, oversight, and leadership, the Department can strengthen relationships among federal, state, and local agencies and benefit from the collective knowledge obtained at all levels of law enforcement in order to combat crime and address emerging threats.

4. Safeguarding National Security Consistent with Civil Rights and Liberties



Source: DOJ OIG

Terrorism continues to pose a fundamental threat to the national security of the United States, along with jeopardizing the peace and safety of individuals throughout the world. Protecting U.S. citizens against acts of terrorism is a top priority in the Department's FY 2014-2018 Strategic Plan, and must continue to be a central focus. FBI Director Comey stated that "the threats posed by foreign fighters, including those recruited from the United States, traveling to join the Islamic State of Iraq and the Levant (ISIL) and from homegrown violent extremists... remain the biggest priorities and challenges for the FBI, the U.S. Intelligence Community, and our foreign, state, and local partners." Recent acts perpetrated abroad by ISIL and al-Qaeda affiliates, as well as domestic acts perpetrated by homegrown violent extremists in Texas and Tennessee earlier this year, demonstrate all too well the need for the Department and its components to remain on guard to try to disrupt this persistent threat.

The Department's proposed FY 2016 budget allocates \$4.4 billion to national security efforts to counter both international and domestic terrorism, improve information sharing and collaboration within the Intelligence Community, counter violent extremism and domestic radicalization, and enhance cybersecurity. Additionally, the ongoing discussions over the government's surveillance efforts and the passage of what is commonly referred to as the USA FREEDOM [Act](#) of 2015 have drawn significant additional attention to the challenge of operating critical national security programs consistent with the public's expectation of privacy. In light of the potential magnitude and serious nature of the threats posed to the public, it is particularly important for the Department to act effectively and aggressively while ensuring that the civil rights and civil liberties of American citizens are protected.

The Department continues to focus much of its efforts on fighting international terrorism. In a June 2015 hearing before the House Homeland Security Committee, the FBI stated that one of the highest priorities for the FBI and the Intelligence Community is to stop homegrown violent extremists, who may be inspired by foreign terrorist ideologies to attack the United States from within. Yet domestic terrorist attacks by individuals motivated by U.S.-based extremist ideologies also remain a serious threat. In response to the threat of domestic terrorism, in 2014 then-Attorney General Eric Holder re-established the Domestic Terrorism Executive Committee to assess and share information about ongoing domestic terror threats. In October 2015, the Department announced the appointment of a new Domestic Terrorism Counsel to serve as the main point of contact for U.S. Attorneys working on domestic terrorism matters. The Department's FY 2016 budget request also includes \$15 million to implement the Countering Violent Extremism Initiative

to address both types of threats to the homeland. It is important that the Department continue to develop and work on these and other initiatives to identify and disrupt potential acts of terrorism – a priority that is particularly crucial in light of a March 2015 [report](#) by the 9/11 Commission that found limited resources and inconsistent implementation of the FBI’s programs to counter violent extremism.

Another challenge for the Department is to prioritize the appropriate sharing of national security information among its components and the Intelligence Community so that responsible officials have the necessary information to act in a timely manner against terrorist threats. Department leadership has publicly agreed and, in its FY 2016 budget request, included additional resources to enhance collaboration with the intelligence community through improved information technology infrastructure and counterintelligence programs. Our ongoing joint review with the Inspectors General of the Intelligence Community and Department of Homeland Security involves oversight of some of these efforts. This joint review is designed to determine whether counterterrorism information is adequately and appropriately shared with all participating agencies, and identify any gaps or duplication of effort in this area.

As the Department continues its important work to protect Americans from national security threats at home and abroad, it must be sure not to impair the civil liberties of those it is protecting. Earlier this year, Congress passed the USA FREEDOM Act, which, among other things, altered the government’s authority to conduct electronic surveillance and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes. The Department must continually strive to achieve the appropriate balance between its national security efforts and respect for the privacy interests of American citizens, a topic the OIG has focused on in some of our national security oversight work. As required by the USA FREEDOM Act, the OIG currently is reviewing the FBI’s use of Section 215 orders under the Foreign Intelligence Surveillance Act (FISA) between 2012 and 2014. This review is examining, among other things, the effectiveness of Section 215 as an investigative tool and the FBI’s compliance with the final standard minimization procedures adopted by the Attorney General in March 2013 for handling non-publicly available information concerning U.S. persons that is produced in response to Section 215 orders. Previous OIG reviews of the FBI’s use of Section 215 orders found that the interim minimization procedures that had been adopted by the FBI in September 2006 did not provide specific enough guidance to agents for the handling of non-publicly available U.S. person information. As a result, the FBI and the Department did not meet the requirements of the statute requiring the Department adopt minimization procedures. However, we found that by 2013 the Department had adopted final minimization procedures for Section 215 materials. The OIG also is 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. This review will examine the FBI’s procedures for retaining, analyzing, and disseminating leads the NSA develops from the metadata, and any changes that have been made to these procedures over time. The review also will examine how FBI field offices respond to leads, the scope and type of information field offices collect as a result of any investigative activity based on those leads, and the role those leads have had in FBI counterterrorism efforts.



Source: DOJ OIG

The Department’s use of other investigative tools to enhance its national security efforts, particularly those involving broad data collection, also requires close monitoring due to the risk of gathering data that is outside that allowed by federal law. In January 2015, a partially declassified version of our September 2012 [report](#) on the FBI’s use of Section 702 of the FISA Amendments Act was publicly released in response to

Freedom of Information Act (FOIA) litigation. Section 702 authorizes the targeting of non-U.S. persons reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. In this report, the OIG reviewed (a) the number of disseminated FBI intelligence reports containing a reference to a U.S. person, (b) the number of U.S. person identities subsequently disseminated, (c) the number of targets later determined to be located in the United States, (d) whether communications of such targets were reviewed, and (e) whether the FBI complied with the targeting and minimization procedures required under the Act. Our report highlighted the challenges inherent in balancing national security interests with civil rights and liberties. In our ongoing work, we continue to evaluate whether the Department is meeting this challenge.

As it employs a variety of strategies to protect the American people from terrorist threats, the Department has the responsibility to ensure that it uses its national security powers both effectively and appropriately, and protects the American people from improper infringements on their civil liberties. The recent public debate over the government's collection of telephony metadata in bulk, as well as the passage of the USA FREEDOM Act to curtail such collection activities, underscores the challenge the Department faces in this area. It must resolve the tension that can exist between national security and civil liberties, striking a balance that will allow the Department to act both forcefully and lawfully in an area where the stakes could not be higher.

5. Ensuring Effective Oversight of Law Enforcement Programs



Source: OJP website

Careful and responsible management of federal law enforcement programs presents a unique challenge to the Department, both domestically and internationally. Many of these programs are not subject to significant public scrutiny, which only heightens the need for effective internal oversight.

One of the Department's constant challenges is balancing the potential risks inherent in its investigative strategies with its law enforcement mission to protect public safety. Perhaps the best recent example of where these two goals can collide was highlighted in our 2012 [Fast and Furious report](#). In it, we found that ATF failed to exercise sufficient oversight of sensitive activities involving firearms trafficking that posed a danger to the public and presented other risks. In response to our review, ATF established a Monitored Case Program to provide greater oversight and coordination of sensitive investigations. We are currently conducting a follow-up review to evaluate the measures the Department and ATF have taken since our 2012 report, including the Monitored Case Program. We are also evaluating the effectiveness of that program in a separate review of several ATF storefront undercover operations that continued or began after the inception of the Monitored Case Program.

Another example where the Department must balance its law enforcement efforts with public safety is in its administration of the Federal Witness Security (WITSEC) Program. The program must ensure the security of witnesses who may be critical to federal prosecutions without unduly increasing threats to the public. Our March 2015 [audit](#) on the handling of sex offenders in the WITSEC Program found that the Department had not used adequate safeguards to protect and notify appropriate law enforcement agencies about the risks posed by these participants. The audit also identified a loophole in the program that left law enforcement

agencies uninformed about certain participants who subsequently left the program. In a May 2013 [report](#), we found that Department components responsible for administering the WITSEC program did not inform the Terrorist Screening Center of new identities provided to known or suspected terrorists in the program, and thus their new, government-provided names were not included on the terrorist watchlist. We currently are conducting a follow-up audit to assess whether this problem continues and determine if the Department has appropriate procedures in place to mitigate the risk to the public.

Monitoring the use of confidential informants poses a similar challenge for the Department’s law enforcement components. While agents rely on their sources to provide valuable information, they also need to make sure the sources do not take advantage of their status and break the law. The level of secrecy necessary for confidential source programs to be successful adds to the difficulty of closely monitoring their use. As a result, the need for components to follow uniform guidelines is essential if Department leaders are to be assured the programs are working as designed. But in our July 2015 [audit](#) of the DEA’s Confidential Source Program, we found that the DEA’s policies did not align with Attorney General Guidelines for reviewing, approving, and revoking a confidential source’s authorization to conduct “otherwise illegal activity” as part of their cooperation with the government. Moreover, we found instances where sources actually were provided Federal Employees’ Compensation Act benefits without appropriate processes in place for reviewing the claims and determining eligibility. We are continuing our examination of the DEA’s Confidential Source Program, and are also conducting a review of ATF’s management of its policies and practices for the identification and approval of confidential informants and its overall oversight of its confidential source program, in order to determine whether these sensitive law enforcement programs are operated appropriately.

Recent tragic events further emphasize the crucial need for effective oversight of law enforcement programs, particularly those that can help curb violent crimes. FBI Director Comey stated after the June 17, 2015, fatal shootings of nine parishioners in a Charleston church that the alleged killer “should not have been able to legally buy that gun that day.” This event brought attention to potential shortcomings in the processes in place for the National Instant Criminal Background Check System (NICS) – which is administered in part by the FBI and provides criminal background checks in support of the Brady Handgun Violence Prevention Act of 1993. The Department must do everything it can to ensure that the background check process works effectively and protects the public’s interests. We are currently auditing NICS to evaluate its effectiveness – among other issues, this audit will focus on how the FBI refers NICS purchase denials to ATF, ATF’s review of those referrals, and whether prosecutions result from this process.

With agents and attorneys stationed in more than 140 countries, the Department also must have effective mechanisms in place to carefully oversee law enforcement personnel working abroad. Our work has shown the problems that result when Department employees do a poor job of representing their agency and their nation overseas. In January 2015, the OIG completed a [review](#) of policies and training governing the off-duty conduct of Department employees working in foreign countries. We found that the Department had not revisited off-duty policies or training in any comprehensive manner since 1996, even though the need for revision had been recognized. We also found that policies and training did not clearly communicate what employees could and could not do while off duty. In response to our report, in October 2015, the Department issued new policies and guidelines governing off-duty conduct and ethics to address the issues we identified as needing attention.



Source: DOJ OIG

Carrying out dangerous law enforcement missions overseas also presents complex challenges for both agents on the ground and their managers back in the United States, particularly if events do not unfold as planned. We are currently conducting a joint review, along with the Department of State OIG, examining the post-incident responses by DEA and Department of State personnel to three drug interdiction missions in Honduras in 2012 that all involved the use of deadly force. This joint review will address many aspects of such international operations, including pertinent pre-incident planning, rules of engagement governing the use of deadly force, and post-incident investigative and review efforts. It will also evaluate the accuracy of information provided to Congress and the public regarding these incidents. Effective management of such dangerous operations is critical to their success, and to the Department's international law enforcement efforts.

Another challenge throughout the Department's law enforcement components is to adequately address and respond to allegations of employee sexual harassment or misconduct. In March 2015, we issued a [report](#) that determined this was an area where the Department needed to focus more attention. This review was conducted in response to congressional inquiries after allegations arose regarding the conduct of U.S. government personnel, including DEA agents, during the President's 2012 trip to Colombia. We found that component supervisors did not always comply with their component policies, and did not report allegations of sexual harassment and misconduct to their respective internal affairs offices, as required. We also found that while the FBI had adequate offense tables to address these violations, ATF, DEA, and USMS did not. Additionally, we concluded that none of the four law enforcement components properly used their offense tables for charging employees with sexual harassment and sexual misconduct offenses. We further found that all four components had inadequate policies and procedures regarding employees sending sexually explicit text messages and images. These failures may hamper the components' ability to conduct misconduct investigations, fulfill their discovery obligations, and deter misconduct. The Department must put in place policies and procedures to ensure that such misconduct by its employees is handled appropriately.

The Department's ability to monitor asset seizure activities, which are often carried out in conjunction with state and local law enforcement, has also gained renewed public attention this past year. These sensitive seizure actions require effective management to ensure that the Department's authorities are used appropriately. For instance, the DEA conducts significant interdiction operations at mass transportation facilities, but our January 2015 [review](#) of the DEA's use of cold consent encounters found that the DEA does not centrally manage or coordinate training, policy, and operational requirements, which contributed to confusion regarding appropriate procedures for these encounters and searches. Our current work includes a review of the Department's oversight of its asset seizure activities, particularly seizures that may be forfeited administratively. This review is also examining the Department's implementation of an Attorney General order, issued in January 2015, that limited the ability of federal agencies to adopt seizures made by state and local law enforcement. Given the risks to civil liberties and public confidence in law enforcement attendant with such activities, the Department must ensure that they are carried out appropriately.

Adding to the Department's oversight challenges is the need to integrate rapidly evolving technologies into rules and policies designed for a pre-digital era. In March 2015, the OIG issued its second audit [report](#) regarding the Department's use of Unmanned Aircraft Systems (UAS), or drones, in law enforcement operations. We identified discrete program management challenges in the FBI's use of drones, and found that the FBI and Federal Aviation Administration (FAA) had drafted rules that expand the locations and times that the FBI could operate its drones without first requesting written FAA permission. In May 2015, the Department issued agency-wide guidance restricting the use of drones to only properly authorized investigations and activities. While the Department has taken steps to formalize its oversight of this particular technology, it must remain vigilant in adapting its management efforts as advanced technological tools, and their use by law enforcement, evolve. In that regard, the Department also recently issued policy guidance governing the use of cell site simulators, sometimes known as "Stingrays." Cell-site simulators

function as cell towers and are used by law enforcement to transmit cell signals – including those from non-target devices – to locate or identify cellular devices in a particular area. The new policy requires Department components to obtain a search warrant supported by probable cause before using cell-site simulators, with exceptions for certain exigent or exceptional circumstances. Use of other technologies to collect and store vast amounts of data, such as that collected by license plate readers, may reveal an individual’s movements or travel patterns. Use of these technologies will require the Department to balance public safety and privacy interests, to ensure these tools are used effectively and responsibly.

6. Promoting Public Confidence by Ensuring Ethical Conduct throughout the Department



Source: DOJ OIG

In order to carry out the crucial mission of enforcing the law, defending the interests of the United States, and protecting the public, the Department’s employees must ensure that their behavior and motives are ethical and beyond reproach. Failure to meet these core expectations undermines the Department’s credibility, presents security risks, and diminishes the Department’s effectiveness.

The Department continues to face challenges in holding all of its senior officials to the highest standards of ethical conduct and must ensure the consequences of wrongdoing are clearly understood. To assist the Department in doing this, in June 2015 the OIG began posting on our public [website](#) summaries of certain high level employee misconduct findings that did not result in a criminal prosecution. This should help ensure public confidence that government employees who commit wrongdoing are held accountable.

Eradicating nepotism and favoritism in hiring throughout the Department remains a challenge for management. In February 2015, the OIG [reported](#) that senior level managers at the International Criminal Police Organization (INTERPOL) in Washington violated the Standards of Ethical Conduct in 2011 and 2012 when they used their positions to benefit friends and acquaintances by placing them in unpaid intern positions that provided

significant advantage when they subsequently competed for paid contractor and full-time positions. The OIG also found that INTERPOL’s Executive Officer exploited his position by working to obtain positions for his son and three others. Separately, an OIG [investigation](#) revealed that in 2014 an Assistant Director at the USMS improperly influenced the hiring of a contract employee with whom the official had a prior romantic and ongoing personal relationship. As we reported in last year’s challenges, in September 2014 the Deputy Attorney General directed all DOJ components to adopt uniform hiring procedures and disclosure forms following two previous OIG investigations that revealed multiple violations of the prohibition against nepotism and other personnel rules. We believe these steps will help reduce nepotism and favoritism in Department hiring going forward, but that the problem persists and the Department must continue to work to address it so that employees and the public understand and believe that hiring is based on merit and not personal connections or other improper considerations.

Strong controls and oversight of law enforcement remain an important issue for the Department as it seeks to maintain its reputation as an organization that prizes integrity. Yet, several OIG investigations in the past year highlight that the Department still struggles to meet different aspects of that challenge. In particular, the Department must remain vigilant in ensuring its employees safeguard sensitive information they encounter in their daily work. The consequences of failures in this area are illustrated by former FBI Special Agent Robert Lustyik, who pleaded guilty to selling confidential law enforcement information regarding a foreign politician for use by his political rival. In March and September 2015, Lustyik was convicted of corruption in two different federal cases and sentenced to consecutive 10- and 5-year prison sentences respectively following separate OIG investigations in Utah and New York. Another ongoing challenge for the Department is maintaining adequate evidence controls to prevent tampering or other agent misconduct, which can undo successful criminal prosecutions. In July 2015, former FBI Special Agent Matthew Lowry was sentenced to 3 years in prison after an OIG investigation revealed that he stole drug evidence while working as an agent between 2013 and 2014. Lowry's misconduct tainted several investigations, requiring prosecutors in the District of Columbia to dismiss cases against more than two dozen convicted drug dealers, and to forego the prosecution of 26 others. Similarly, the Department must also implement controls to prevent employees from inappropriately enriching themselves with Department funds. A former DEA employee was sentenced to 2 years in prison and ordered to pay restitution in the amount of \$113,841 after an OIG investigation revealed she had applied for and used credit cards issued to fictitious DEA employees. And the Department must also closely monitor undercover operations, particularly those in emerging areas. This challenge is exemplified by former DEA Special Agent Carl Force, who pleaded guilty to extortion, money laundering, and obstruction of justice in connection with his theft of \$700,000 in bitcoins, a form of electronic currency. Force stole the bitcoins while working undercover, as part of the multi-agency Electronic Crimes Task Force, to investigate the Silk Road, an online marketplace selling illegal drugs and other contraband.

A valuable resource for the Department in combating these challenges are whistleblowers, who perform a critical public service in bringing to light information that safeguards the Department against fraud, waste, and misconduct. The OIG remains committed to supporting the efforts of whistleblowers and ensuring that they are fully aware of their rights and protections from reprisal.



Source: DOJ OIG

For FBI employees, there is a separate regulatory scheme through which whistleblowers pursue allegations of reprisal within DOJ. However, a January 2015 [report](#) by GAO found that there was significant room for improvement in the Department's process, particularly with regard to the scope of the persons to whom disclosures can be made and be considered protected,

and the timeliness of the Department's handling of these important matters. At the OIG, the number of FBI whistleblower retaliation complaints has risen dramatically in recent years. This increase will likely accelerate in the future due to the OIG's expanded training and education efforts, including partnering with the FBI to create a new mandatory training program for all FBI employees, as well as a recent DOJ proposal, supported by the OIG, to increase the list of officials to whom protected disclosures may be made under the FBI whistleblower regulation. The Department will face a growing challenge in handling an expanding docket of these matters in a timely fashion so that any appropriate remedies are not rendered moot by the passage of time or otherwise.

For the Department's leaders to be effective in managing agency programs, they must be able to rely on accurate, real-time information regarding which programs are working and which need improvement. But as recent experience has shown, those goals can be thwarted if the Department denies or delays the OIG's access to all of its records, as required by the Inspector General Act. In recent years, several OIG reviews were delayed by Department components that withheld certain information requested by the OIG, including (a) an evaluation of how the Department's law enforcement components handled sexual harassment

allegations, (b) an audit of the DEA's policies and oversight over its higher risk confidential sources, and (c) a multi-agency review of the government's sharing of information leading up to the Boston Marathon bombing. For Department leadership to be able to benefit from the OIG's work in improving the integrity and efficiency of the Department's operations, our office must be able to engage in independent oversight. This also fosters public trust in government. In July, the DOJ Office of Legal Counsel (OLC) issued an opinion concluding that the Inspector General Act did not authorize the DOJ OIG to have independent access to grand jury, wiretap, and certain credit information. Immediately following the issuance of OLC's opinion, the OIG requested that Congress promptly pass legislation, supported by the entire IG community, to ensure that Inspectors General have independent access to the information they need to perform their critical duties. Both the Attorney General and the Deputy Attorney General have expressed their support for this effort and the Department should make every effort to ensure this important principle remains at the core of the law that ensures IGs can perform their critical duties.

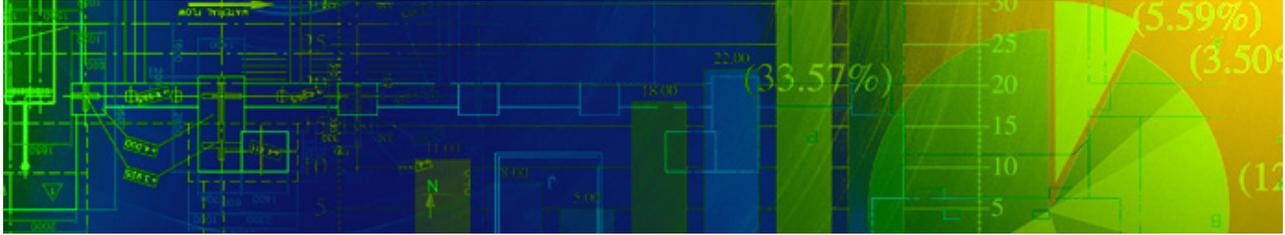
Another issue that continues to draw widespread scrutiny is the process for how the Department handles complaints regarding the conduct of Department attorneys when they are acting as such. A December 2014 GAO [report](#) found the Department does not do enough to ensure that attorneys who have engaged in



Source: DOJ OIG

professional misconduct serve the discipline imposed. The GAO report acknowledged that the Executive Office for U.S. Attorneys (EOUSA) revised its procedures for documenting attorney discipline after a February 2014 OIG [review](#) of that component's flawed disciplinary system. But the GAO report also found that poor recordkeeping still hampered EOUSA's ability to ensure that discipline decisions were consistent and that discipline was actually imposed. More fundamentally, the GAO report also noted that Congress and others, including the American Bar Association, continue to voice concerns that the Department's underlying process for disciplining attorneys lacks transparency. The GAO report noted that some members of Congress have called for the OIG to have jurisdiction over professional misconduct investigations against DOJ attorneys on the grounds that the OIG's statutory and operational independence from the Department would better ensure that sufficient and timely information on attorney misconduct is provided to the public. Similarly, the independent, non-partisan Project on Government Oversight called in a March 2014 report for jurisdiction over

attorney misconduct within the Department to be transferred to the OIG, just as it exists at other agencies throughout the federal government, based on our statutory independence and transparency. As mentioned above, the OIG regularly posts summaries of employee misconduct findings on its website, including those involving Assistant U.S. Attorneys. By contrast, the Department's Office of Professional Responsibility (OPR), which has exclusive jurisdiction to investigate Department attorneys for alleged misconduct arising from litigation-related activities, discloses only summary data and examples in its Annual Reports, and the most recent annual report available on its public website describes misconduct that occurred more than 2 years ago. The Department faces a significant challenge in ensuring the public credibility and transparency of investigations of its attorneys who are themselves at the forefront of carrying out the laws.



Source: COPS website

7. Effectively Implementing Performance-Based Management

Performance-based management continues to be a challenge for not only the Department, but also the entire federal government. The Government Performance and Results Modernization Act of 2010 (GPRA) and corresponding guidance in the Office of Management and Budget’s Circular No. A-11 emphasize priority-setting, cross-organizational collaboration to achieve shared goals, as well as the use and analysis of goals and measurements to improve outcomes. GPRA also requires federal agencies to establish priorities, conduct quarterly data-driven reviews to measure performance, and use Performance.gov as a vehicle to report this information to the public. As the Department implements these GPRA requirements, it must work to develop, collect, and analyze meaningful and outcome-oriented performance metrics.

The Department has over 40 components that administer programs with a wide range of important goals, including prevention of terrorism, promotion of national security, reduction of violent crime, and enforcement of federal laws. Measuring programmatic outcomes is frequently not easy with these types of programs, but the Department must continue to develop the means to identify and collect data related to performance measures. In short, collecting the right data, and then using it to evaluate performance and improve management of programs, will aid the Department in accomplishing its strategic goals.

The Department has begun implementing the tenets of performance-based management with the development of four priority goals and a focus on results that can be accomplished within 12 to 24 months. The Department reported to the public, via Performance.gov, that as of March 2015 it exceeded all priority goals in the areas of national security, violent crime, and financial and healthcare fraud, while noting it still needed to do more to protect vulnerable victims. However, our work has found that the Department must improve the reliability of the data it collects and must better analyze this data to improve its tracking and assessment of operational performance.

Many of the Department’s current performance goals and indicators focus on inputs, workload, or processes, rather than focusing on outcomes and results. For example, several of the Department’s performance measures, such as the reduction of the number of financial and healthcare fraud investigations pending longer than 2 years, focus on workload as opposed to outcomes. While they may provide information about the number and duration of financial and healthcare fraud investigations, these measures fail to convey the significance and impact of the Department’s efforts to reduce these types of crime. Results-oriented measures are critically important if the Department is to effectively monitor whether its programs, initiatives, and operations are accomplishing their intended goals. The Department must capture information that meaningfully links its inputs to outcomes in order to properly direct its efforts and show the value of its programs to taxpayers.

As an example, a June 2015 GAO [report](#) found that while the Department has created “key indicators” intended to measure the success of its Smart on Crime initiative, these indicators generally do not show whether the Department is making progress toward the initiative’s goals. Specifically, the GAO found that

7 of the 16 indicators are confusing or do not represent the information the indicator name implies, and that 13 of the 16 indicators lack contextual information needed to appropriately interpret their results. In the same report, the GAO reviewed the performance measures for the Department's Clemency Initiative and reported that, even though the goal is to expeditiously process clemency petitions, the Department is not tracking how long, on average, each step in the review process takes. In addition, the GAO concluded that the BOP does not have a comprehensive plan in place to gauge the success of the nearly 20 reentry programs designed to reduce recidivism. Research indicates that improved data collection and clearly defined goals and progress measures can assist agencies such as the Department in more effectively measuring their efforts.

Our work has also identified repeated instances where the Department does not collect the right information needed to inform program decisions and therefore struggles to make meaningful program improvements. For example, our January 2015 [review](#) of the DEA's cold consent encounters at mass transit facilities found that task force agents do not collect demographic information about each encounter they conduct or encounters that do not result in drug or money seizures. As a result, the DEA cannot assess whether it is conducting these encounters in an unbiased or effective manner. We identified another example of inadequate data collection and analysis during our November 2014 [audit](#) of the Department's international fugitive removal efforts. In this audit, we found that the Department should adopt a fully-informed decision-making process that considers several factors including the cost of bringing an international fugitive to the United States to face justice. However, we found that the USMS did not maintain complete and accurate cost data associated with its international fugitive removal efforts and, therefore, could not do this. Findings such as these indicate a continued need for the Department to embrace performance-based management by asking the right questions that generate data directly relevant to the requirements and goals of its programs.

Reliable data is an essential building block to effective performance-based management and has proven to be elusive at times for the Department. In its 2014 Annual Performance [Report](#), the Department said it views data reliability and validity as critically important in the planning and assessment of its performance and that every effort is made to ensure the completeness and reliability of its data. Yet, the OIG continues to find examples where the Department has failed to collect accurate and reliable data. As the Inspector General noted in recent testimony before Congress about the BOP, the absence of reliable data impinges on the OIG's mission as well as the Department's ability to evaluate the effectiveness of its programs and to make necessary improvements. For example, during several of our reviews, the OIG was unable to obtain recidivism data from the BOP for federal inmates. If it had better data, the Department could better focus its limited resources and make strategic investments in programs that show progress in reducing incarceration costs, deterring crime, and improving public safety.



Source: DOJ

Further, the OIG has found that on many occasions when the Department does try to collect data, the data is inaccurate, unreliable, or simply goes unused, thereby impacting its ability to effectively manage and assess its operations. For example, our June 2015 [review](#) of the U.S. Attorneys' Offices' (USAOs) debt collection program found insufficient data entry controls for the Department's debt collection tracking system. As a result, the system did not contain sufficiently reliable information to enable the USAOs and the Executive Office for U.S. Attorneys (EOUSA) to accurately assess the performance of their Financial Litigation Units and the debt collection program as a whole. This deficiency was coupled with the failure of the debt collection tracking system to capture all the information needed to sufficiently evaluate debt collection performance across the USAOs. As a result, the USAOs and the EOUSA could not rely on the data they collected to inform management decisions for the USAOs' debt collection program. This report also identified staffing issues that limited the ability of Assistant U.S. Attorneys to track debt collection matters. Given that the U.S. Treasury is owed more than \$1 billion, it is important that the Department prioritize its data collection in this area so it can better track down the money the federal government is owed.

Having accurate metrics, good data, and strong analysis is valuable, but if the Department does not have enough talented personnel to carry out its goals, its program performance inevitably will suffer. To improve its performance, the Department needs to do a better job investing wisely in human capital. Since January 2011, the Department has had to operate with fewer staff for many reasons, including budget constraints and difficulties in the hiring process. A January 2014 GAO [report](#) found that 28 percent of employees working for the Department in 2012 will be eligible to retire by September 2017. In light of the Department's request to Congress for funding to add 580 positions during FY 2015 and another 1,598 positions in FY 2016, it needs to find strategies to ensure that it is wisely planning for new hires and investing in human capital so that programs have the personnel they need to be successful.

Performance-based management remains an ongoing challenge for the Department. Improving the Department's collection and analysis of program performance measures is critical, as is collecting more reliable data. Enhancing these areas will assist the Department in more effectively measuring its programs and allocating its resources, and as a result, achieve more of its strategic management goals. The OIG is taking steps to apply data analytics models to Department data with the goal of better assessing the effectiveness and efficiency of the Department's programs and operations, along with improving the OIG's ability to identify waste, fraud, and abuse. However, the success of the OIG's efforts will depend, at least in part, on the quality and relevance of the data the Department collects.

8. Protecting Taxpayer Funds from Mismanagement and Misuse



Source: Office for Victims of Crime website

With an FY 2015 budget of \$26.2 billion, the Department must act as a responsible steward of not only the funds it uses internally but also funds it distributes to outside parties through contracts and grants. To ensure that it earns the public's trust, it is imperative that the Department diligently protect taxpayer funds, manage its own resources wisely, and seek ways to improve the economy and efficiency of agency programs.

The Department faces significant challenges in using and monitoring funds within its control. In FY 2015, the OIG's audit-related efforts resulted in 79 reports that contained approximately \$53 million in questioned costs, reported over \$4 million in funds that should be put to better use, and made more than 300 recommendations for management improvements. Our work has highlighted shortcomings in the Department's management and oversight of tax dollars – particularly funds distributed through contracts and grants. Our reports show this remains a continuing challenge for the Department.

Funds Spent within the Department

The Department expends millions of taxpayer dollars on its internal operations and programs and must handle these funds efficiently and responsibly. Yet, recent OIG work has shown that there is room for improvement in the Department's management of its spending in a wide variety of areas. For example, in the OIG's [audit](#) of the Department's use of extended Temporary Duty (TDY) travel, we found that the FBI, Criminal Division, National Security Division, and the Executive Office for United States Attorneys and U.S. Attorneys' Offices, made extensive use of extended TDY. Based on the limited data available, we estimated that these components combined spent more than \$54 million on 4,788 extended TDY events between FY 2012 and the first quarter of FY 2014. However, we found that the components are not adequately tracking extended TDY, and that they may be inappropriately relying on it to respond to staffing or other issues, using it when it is not warranted and not using it when it is. Similarly, the OIG's March 2015 [audit](#) of the Department's Unmanned Aircraft Systems (UAS) provided another example of poor fiscal management.

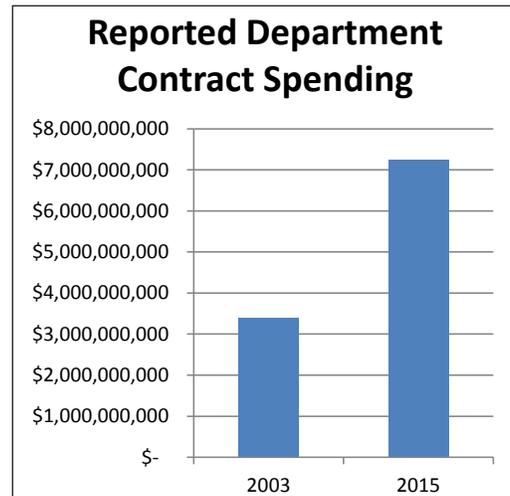
We found that ATF spent approximately \$600,000 on UAS vehicles (commonly referred to as “drones”), but never flew them operationally. We also found that less than a week after ATF suspended its UAS program in June 2014 and disposed of its drones, a separate unit within ATF purchased five small commercial drones for approximately \$15,000 without coordinating with ATF’s UAS program office.

More broadly, the Department faces a significant challenge ensuring that it puts in place policies and procedures sufficient to make its stated commitment to collecting federal criminal and civil debts – the principal balance and interest on which totaled some \$114.6 billion in FY 2014 – into a reality. In a [report](#) reviewing the debt collection program of the U.S. Attorneys’ Offices, the OIG found that, despite acknowledging the importance of this effort, the USAOs failed to prioritize debt collection activity, which resulted in insufficient attorney and support staffing and ineffective collaboration within the USAO, thereby hindering collection efforts. If the Department is to effectively manage its budget in times of limited funding, it cannot afford to fail in this important area.

Despite these challenges, the Department has made important progress controlling costs in other areas, as shown by the OIG’s most recent [report](#) on Conference Planning and Reporting Requirements. Between FY 2010 and 2014, DOJ conference costs fell by about \$72 million, as the number of conferences attended fell from 1,740 to 445. This is one example of how, across all components, the Department should continue to identify ways to run its programs more effectively and efficiently.

Funds Spent via Contracts and Grants

Given the scope of its procurements and awards, the Department also faces a vast oversight challenge as it seeks to ensure that it awards contracts and grants wisely and judiciously, and that the recipients use these funds to achieve their intended purpose. According to data from the government’s USAspending.gov website, Department spending on contracts with outside companies increased dramatically over the past decade, more than doubling between FY 2003 and FY 2013. The exposure of such widespread government contracting remains real given the Department reportedly spent over \$7 billion on contracts during FY 2015. This requires vigilant and continuous risk-based management and oversight of the Department’s contracts. The primary responsibility for performing this function inevitably rests with the Department, though to help ensure that this occurs, the OIG continues to hire personnel with specialized knowledge about government contracts to help it monitor the Department’s efforts in light of the significant tax dollars spent in this area.



Source: USAspending.gov

One area of significant exposure where the OIG has recently focused attention is the Department’s use of high-dollar contracts to run privately-managed prisons, which housed approximately 24,000 inmates, or 12 percent of the BOP’s inmate population, as of September 2015. In April 2015, the OIG issued a [report](#) on the Reeves County Detention Center in Pecos, Texas, one of BOP’s largest private prison contracts, questioning its use of \$2 million and its plans for unnecessarily spending another \$1 million. Currently, we are also conducting two audits of contracts for prisons operated by the Corrections Corporation of America (CCA) – the BOP contract award to CCA to operate the Adams County Correctional Center in Natchez, Mississippi, and the USMS contract awarded to CCA to operate the Leavenworth Detention Center in Leavenworth, Kansas. We are also conducting a broader review of the Department’s efforts to monitor its extensive use of contract prisons. The Department must ensure that these funds are spent wisely and result in institutions that are safe and secure.

Grant funding also continues to present a significant risk for mismanagement and misuse due to the sheer volume of recipients and money involved, along with program objectives that are often hard to quantify and results that are not adequately measured. According to USAspending.gov, from FY 2010 through FY 2014, the Department awarded approximately \$13 billion in grants to thousands of recipients. Our recent OIG work has identified several instances when Department components exercised limited monitoring of grants and conducted few site visits. Additionally, we have found further breakdowns in monitoring at the subgrantee level, when grant recipients distribute the funds to third parties and do not adequately ensure they fulfill grant conditions. The Department must undertake robust efforts in this area to ensure that the billions it gives out in grants are appropriately spent and that the public receives the expected and desired return on its investment.



Source: DOJ OIG

One particular area where the Department will face increased responsibility is in its management of the Crime Victims Fund (CVF). In December 2014, Congress authorized the Department to use up to \$2.36 billion of the current CVF balance. This more than triples the amount of CVF funds the Department was authorized to expend compared to FY 2014. This increase will allow the Department to distribute significantly more CVF grant funds through victim compensation and assistance grant programs. The OIG currently is auditing the Department's risks in managing the increase in CVF grant funds and we anticipate being active in auditing those receiving the CVF grants in the future. But the challenge remains for the Department to effectively and efficiently manage such vast expenditures in order to ensure that the goals Congress set for these grants are met in a timely fashion.

The Department's failure to effectively oversee grant awards was exemplified in an [audit](#) of grants awarded to the Navajo Division of Public Safety by the Office of Justice Programs, Bureau of Justice Assistance. In that audit, we found \$35 million in questioned costs focused on the construction of correctional facilities in two Arizona locations with capacities that were at least 250 percent larger than needed. Similarly, the OIG's [audit](#) of \$77.5 million in grants to the Puerto Rico Department of Justice (PRDOJ) questioned over \$5 million, including millions in funds that were drawn down and not expended and others that were never used, despite the difficult economic and criminal justice challenges on the island. We also found that the PRDOJ failed to accomplish a significant portion of the grant-funded projects, something the Department failed to identify or address.

These are just examples, but the lesson is clear: both contracts and grants continue to present significant management and oversight challenges for the Department, and it must find new and better ways to interact with funding recipients to ensure that funds are expended for their stated purposes. At the most extreme end of the spectrum the OIG's Fraud Detection Office has uncovered issues including improper consultant payments, conflicts of interest, and embezzlement, affirming the need for vigilance in these areas. The OIG conducts integrity briefings for thousands of participants every year to help bring these issues to the fore, but it is ultimately up to the Department to ensure that its funding is spent responsibly.

This page intentionally left blank.

**MANAGEMENT'S RESPONSE TO THE FY 2015
OFFICE OF THE INSPECTOR GENERAL'S REPORT ON THE
TOP MANAGEMENT AND PERFORMANCE CHALLENGES
FACING THE DEPARTMENT OF JUSTICE**

The Department of Justice is the world's largest law office and the central agency for enforcement of federal laws. The Department's mission and responsibilities extend over a broad spectrum, and this obligation includes many challenges. This year's Office of the Inspector General's (OIG) report recognizes the progress the Department has made in addressing the many of its challenges, and the Department appreciates this recognition.

1. Achieving Balance and Containing Costs in a Significantly Overcrowded Federal Prison System.

Although the number of federal inmates has declined for a second year, the federal detention and prison spending remains a large share of the Department's budget due to the overall size of the inmate population. The Department continues to look for ways to safely house inmates while managing rising costs.

The Federal Bureau of Prisons (BOP) continues to work on recruiting and filling Correctional Officer positions at all facilities, in particular at the Medium and High Security levels. BOP continues to examine all mission critical posts and realign staff to ensure adequate coverage is provided within resources. Recognizing the risk of violent offenders at high security prisons, BOP included a request for 714 additional correctional officers for housing units at the High Security level in the FY 2016 President's request. BOP has established a National Recruiter Position to work with Regional Recruiters, Human Resource Managers, and Diversity Management staff to expand and enhance recruitment efforts in all disciplines.

BOP agrees with the OIG that while contract prisons help alleviate overcrowding at BOP facilities, they are a short term solution. The Department acknowledges while there was significant property damage at the privately run Willacy Correction Center earlier this year, the staff injuries reported were not serious.

Restrictive housing plays an important role in helping BOP operate safe, orderly, and humane institutions. Although BOP always seeks to place inmates in the least restrictive setting possible, there are some cases where a prisoner poses a threat to the safety and security of prisons, or requires protection from other inmates, and therefore must be housed in a more controlled environment. BOP continues to review its policies in this area, with a particular focus on identifying the safest and most psychologically appropriate way to house inmates with serious mental illness (SMI) who cannot function in general population and who may pose a serious danger to other inmates and staff. BOP has recently implemented numerous policy changes to enhance the care and treatment of prisoners with SMI, including the creation of residential mental health treatment units at the United States Penitentiaries (USP) in Atlanta, Georgia and Allenwood, Pennsylvania, as well as a residential treatment unit at the USP in Florence, Colorado for inmates with borderline personality disorders. The Department remains committed to continuing to review these policies and practices.

BOP continues to implement new advanced technology to combat the introduction of contraband. BOP was the first corrections entity to install the CEIA 601 Plus Walk-Thru Metal Detectors, which have a higher sensitivity to stainless steel, aluminum, and ferrous metals which can be networked to better identify the presence of contraband. BOP deployed units to 18 penitentiaries and installed 123 SecurPass Whole Body Imaging devices at institutions, which can be effectively used during intake screening to determine if inmates have contraband secreted inside their body cavities. BOP has deployed thermal fencing at sites where contraband was previously introduced at the fence line. The thermal fencing has proven effective at detecting when persons attempt to scale or throw contraband over the fence, but also effective in alerting staff in real-time so those persons can be arrested onsite. BOP continues to explore cellphone detection devices and other contraband detection technology.

Containing the Cost of the Federal Prison System

As noted in previous reports, medical costs are a primary driver in the increase in prison expenditures. The aging prison population is a growing consumer of medical services. The Department and BOP have and will continue to implement all prudent mechanisms to reduce these healthcare costs without sacrificing the appropriate standard of care.

The report states that BOP's budget increased by 11 percent from the FY 2009 level. During the same time period, the inmate population increased every year except for FY 2014 and FY 2015. Also during that same time period, the BOP experienced dangerously high levels of crowding particularly at higher security institutions. Through increased resources for additional staff and newly activated institutions, BOP enhanced institution safety and security while reducing dangerously high crowding levels.

BOP's budget supports critical funding for inmate programs that have proven to reduce recidivism and thus limit future incarceration costs. BOP's ability to provide inmates with these vital programs is contingent upon adequate funding levels to support the salaries and benefits of the staff that conduct these programs. BOP has a significant number of inmates on waiting lists for most of the available inmate programs, including General Educational Development (GED) classes. The GED program currently impacts 35 to 40 percent of the BOP population and has a backlog of more than 10,000 inmates waiting to participate in the program. With the inmate population declining, BOP will be better able to offer programming to inmates and reduce waiting lists. However, BOP is faced with rising costs of GED programs that are now administered via computers and offered in Spanish. The cost of keeping computer equipment and other resources modern is necessary in order to align the program with community standards. BOP would like to increase the programs that support successful reentry into the community and ultimately reduce recidivism among inmates.

The OIG recognized in their report medical costs and aging prison populations are major factors in BOP's overall rising costs. It should be noted that the increases in BOP health care expenditures are analogous to industry-wide increases, but on a significantly lower scale. For example, the per capita health care cost for BOP in FY 2014 was \$6,176 while the per capita National Health Expenditures rate reported by the Centers for Medicare and Medicaid Services for 2013 was \$9,255. BOP enters into contracts for medical specialty services which cannot be provided within prison clinics because it would be cost-prohibitive to hire the variety of medical specialists needed. OIG does not acknowledge the industry-wide increases in health care costs, nor the challenge of recruiting and retaining medical staff in remote locations, a shrinking health care labor market, and the difficulty to compete with industry salaries for many health care professions.

Properly Evaluating Other Department Programs and Policies Can Better Address the Prison Crisis

The Department is working to isolate and contain the growing operational costs and frequently looks beyond BOP to each component to offer assistance with cost cutting ideas.

The Government Accountability Office noted in a 2014 report the Department could save over \$4 billion in the next several years through retroactively reducing prison sentences, a statement to which the Department concurs. As part of the Smart on Crime initiative, the Department announced approximately 6,000 non-violent drug offenders will be released early from prison. The release of these is anticipated to occur between October 30 and November 2 and the U.S. Sentencing Commission estimates more than 8,000 defendants will be eligible for release the following year. Since the BOP expanded its Compassionate Release program in 2013, the number of federal inmates released under the program has increased significantly. For example, between January 2013 and November 2015, the BOP approved 242 inmates for compassionate release, a marked increase from 2012 and 2011, when only 39 and 29 inmates were approved for release under this program, respectively. The BOP works to ensure that if an inmate sufficiently meets all of the stated criteria and does not pose a known risk to the community, he or she is recommended for compassionate release. The Department continues to assess the effectiveness of the Compassionate Release program.

Since the initial review of the International Prisoner Transfer Program in 2011, the Department has expended considerable effort and made significant progress to improve the program, including, as the OIG acknowledges, increasing the number of applications and improving the overall management of the program. The Department fully concurs with all recommendations set forth in the August 2015 follow-up report and has taken steps to implement them. It is important to recognize that the voluntary nature of the transfer program, the lack of treaty agreements with all foreign countries represented by the foreign national inmate population, and restrictive criteria imposed by treaty nations significantly limit the number of inmates eligible for transfer. Even after the Department has approved the application of eligible inmates, the number transferred may be limited because receiving countries may still deny the transfer or fail to provide a decision in time to make transfer of an inmate practicable. Nonetheless, the Department remains committed to increasing the number of approved transfers.

The Department agrees that identifying additional data collection opportunities and developing new data indicators to incorporate into Smart on Crime performance measures will help better achieve the goals of this initiative. The Department has already commenced discussions with the U.S. Sentencing Commission on new, more granular data elements and hope to incorporate those elements into our indicators in the coming months. In addition, the Department is incorporating regular BOP population, staffing data and estimates into relevant indicators. While measuring data and indicators for the Smart on Crime initiative is important, the Department also believes that prosecutors should investigate and charge federal crimes when justice and public safety demands it. And prosecutors should and will make these individualized decisions without concern for the overall federal prison population, without concern for a charging decision's effect on a "measurable target," and without concern for any other incentive. The Department remains actively engaged on this issue.

2. Enhancing Cybersecurity in an Era of Increasing Threats.

Cybersecurity attacks, including from criminals, terrorists, and nation-states and their agents, are considered a major national security and public safety threat. In order to protect the Nation from cyber-threats, the Department has adopted a comprehensive approach that is built upon the full spectrum of its criminal and national security authorities, tools, and capabilities. The Department investigates and prosecutes large-scale data breaches, transnational criminal cyber organizations, terrorists, and nation state actors, and other categories of hackers who deploy sophisticated tools to steal from and damage computer networks. Additionally, the Department develops and implements national cyber policies and regularly collaborates with agencies within the intelligence and defense communities to detect, deter, and interdict cyber threats before they become actual events or criminal cases.

The Department agrees with many of the challenges identified by the OIG in its report, particularly with the value of developing and implementing a cohesive strategy to address cyber security. In 2014, the Department developed a multi-year cyber threat strategic plan, and continues to refine its cyber strategy to ensure that its structure, activities, and vision are up-to date to confront the dynamic threats identified by OIG. The Department's Criminal Division (CRM) launched the Cybersecurity Unit in December 2014 to ensure that the cybersecurity expertise that resides in the Division's Computer Crime & Intellectual Property Section (CCIPS) supplements government-wide efforts to make computer networks more resilient and data more secure. The Cybersecurity Unit works closely with National Security Division (NSD), and the United States Attorney Office (USAO) community to maximize the impact of the Department's cyber security efforts.

In order to improve the ability of federal prosecutors to deter, detect, and disrupt cyber threats, EOUSA's Office of Legal Education continued to host training courses throughout the year. These courses are prepared and taught by leading experts from NSD, CCIPS, the USAO community and outside experts and are designed to directly address issues with investigations and prosecutions in cybersecurity. During FY2015, these courses included, among others, the Computer Hacking and Intellectual Property Prosecutors Training and the National Security Cyber Specialist (NSCS) Training. The NSCS network, established in 2012, coordinates

the responses to cyber threats — including economic espionage and trade secret theft — being conducted by nation-state actors or terrorists, or in a manner that otherwise significantly impacts national security. Each USAO has at least one Assistant United States Attorney (AUSA) assigned to the NSCS network who provides technical and specialized assistance to his or her colleagues within the district and is a point of contact for NSD and CCIPS for information sharing, outreach, and de-confliction purposes.

To recruit and retain highly-qualified cyber-skilled candidates, the FBI has launched several initiatives, including partnering with academic institutions known for computer science and computer engineering programs to identify students with the necessary skills to help the mission of the FBI's Cyber Division. Additionally, the FBI has partnered with professional and trade associations in these fields as well as with professional training groups to identify individuals who have worked in this industry and have practical field experience. To more actively target candidates, the FBI has also created new marketing and recruiting materials and tools and has conducted a more targeted approach of scientists and engineers.

Encryption is increasingly present within the tools and techniques utilized by malicious actors encountered throughout law enforcement. When properly implemented, encryption has the unique ability of enabling criminals to operate in plain site without risk of being caught because encrypted data is obscured from potential victims and law enforcement. While the Department understands consumer concerns about privacy, law enforcement must also have the ability to lawfully access plain text in order to successfully isolate and mitigate cyber threats. DOJ encourages the use of managed encryption, which applies strong encryption in a manner consistent with industry best practices, but which also allows for decryption if illegal activity occurs. The Department also encourages development of new multi-party encryption standards, which could secure data in a manner consistent with industry best practices, and requires multiple parties to agree in order to allow for decryption by providing their portion of encryption keys. These new standards could mitigate perceived weaknesses of current managed encryption practices.

The Department strongly agrees with the OIG that effective partnerships outside of the federal government are critical to confronting the cyber threat. DOJ conducts outreach to inform companies and the general public about nascent threats and DOJ works with other federal departments and agencies to inform companies and individuals that they have been victimized so that they can better protect themselves. The Department collaborates with both Intelligence Community (IC) and law enforcement partners to share cyber threat information with the private sector. Within the FBI's Cyber Division, the Cyber Outreach Section proactively developed trusted partnerships with many private sector companies and industry associations and is able to share timely information and grow relationships, particularly focusing on dispelling misconceptions regarding privacy concerns. The FBI coordinates investigative and operational responses to cyber events, and disseminates messages containing intelligence and threat indicators to both IC partners and the private sector, when appropriate. The FBI also helps to coordinate the Government's response to computer intrusion activity and notification of victims.

In the past year, NSD announced strategic changes designed to put additional focus on the protection of national assets from the threats of nation states, including cyber threats. These changes included creating a new Deputy Assistant Attorney General position focusing on protecting national assets and naming the first Director of the Division's Protection of National Assets Outreach Program. Pursuant to this increased focus, NSD leadership and other attorneys have reached out to senior managers and counsel at hundreds of companies over the last year to educate them about the Department's resources and efforts to combat economic espionage and trade secret theft and other national security threats. These outreach efforts have included presentations at universities and think tanks, cybersecurity summits and roundtable discussions, as well as one-on-one meetings with senior executives at Fortune 500 and other companies. NSD's National Cyber Security Specialists Network also periodically disseminated resources to its members nationwide to facilitate their outreach to companies and other organizations in their home districts and facilitated FBI field offices' efforts to educate AUSAs on the national security threats in their districts and to include them in FBI's outreach efforts in their districts. The USAO community and the CRM also conduct public and industry

outreach and awareness activities.

To further enhance international law enforcement cooperation during FY 2015 the FBI expanded its Cyber Assistant Legal Attaché (ALAT) program. Cyber ALATs are embedded with foreign host nation law enforcement or intelligence agencies to facilitate information sharing, increase cooperation on investigations, and improve relationships with foreign partners. FBI also established the Internet Cyber Crime Coordination Cell (IC4) to bring together the most significant international and domestic partners in the fight against cybercrime and house them in one space at Mission Ridge in Chantilly, Virginia. The Mission Ridge facility will allow domestic and international partners to have permanent subject matter expert detailees placed within IC4 and is designed to allow detailees to have connectivity to their own agency's databases.

Safeguarding the government's systems, data, and personnel is of great importance to the DOJ mission; as shown through our progress on mandatory Personal Identity Verification (PIV) implementation during the past year. We have instituted greater rigor in our compliance tracking by moving away from manual self-reporting to leveraging automation to capture mandatory PIV adoption in real time. During the third quarter of FY 2015, one of our Components underwent a major infrastructure upgrade, we introduced new hardware and software along with the retirement of legacy systems, and we adjusted our total user count by adding an Intelligence Community Component to the totals; these actions together accounted for the temporary decline in our PIV metrics. However, by year-end, not only has this temporary dip been restored, but the Department has also achieved a major milestone with Bureau of Prisons reaching 100% mandatory PIV login. By the end of the fourth quarter, the Department's overall percentage was 64% mandatory PIV card compliance, which is a substantial improvement over the FY2014 end-of-year result of 29%.

The Department is committed to closing the gap on PIV compliance. This effort, especially with a organization our size, requires continuing investment and focus to ensure that mandatory PIV adoption, including any backend infrastructure and physical access requirements, are fully implemented at all Components and all field offices. We are working with the last remaining Components to develop appropriate plans of action and milestones that will move DOJ to the forefront of PIV usage.

DOJ has successfully leveraged OMB's Cross-Agency Priority (CAP) goals and FISMA metrics to enhance our efficiency and effectiveness in detecting and mitigating security weaknesses. For example, based on FISMA requirements, DOJ implemented an automated asset, configuration and vulnerability management solution across the entire enterprise. The Department has a centralized and near real-time view of our cyber security posture synthesized into an effective risk management dashboard for our executives' use. This dashboard captures where each of the 40 component agencies and offices stand in terms of quantity and types of assets, their vulnerability exposure as measured by outstanding patches and software versions, and the degree to which the environments are hardened based on their secure configuration baselines. DOJ has successfully transformed this FISMA compliance requirement into an effective tool to provide actionable intelligence, and reduced the Department's overall vulnerability footprint by over 50%.

DOJ strives to stay abreast of cybersecurity issues and improve the protection of its critical systems and information from attack and compromise. One of the major areas of focus for our continuous monitoring program is the identification of out-of-date software and its subsequent retirement or upgrade. These legacy systems are difficult to patch, do not easily accept automated monitoring and reporting, and frequently cannot utilize the most up-to-date software.

DOJ and its Components historically have worked together with OIG on its FISMA system assessments. Previous year plans of actions and milestones mitigation plans remain outstanding and DOJ continues to work closely with each affected Component to validate the plans and schedule for resolution and help remove impediments to closure. When OIG issues the reports and recommendations for FY 2015, we will coordinate with each affected Component to develop strong and actionable plan of action and milestones along with an agreed upon timeframe for resolution for each new finding. This proactive approach will improve the Department's cybersecurity posture and allow it to be better prepared to prevent intrusions.

3. Building Trust and Improving Police-Community Relationships.

Recent police-involved shootings and other use of force incidents in places like Baltimore, Maryland, Ferguson, Missouri, and New York City offer a stark illustration of the ongoing need to bridge the gap between law enforcement and the communities they serve and to bolster effective, accountable policing in all communities. Consequently, the Department devotes substantial resources to ensuring that policing is done in accordance with the Constitution, and to help local police departments and the communities they serve build trust where it has eroded.

The Department recognizes that the role of law enforcement is not only to enforce the law, but also to preserve the peace, minimize harm, and sustain community trust. DOJ's grant-making components oversee many successful programs that foster partnerships with state and local law enforcement agencies: OJP's National Initiative for Building Community Trust and Justice, an Administration priority, aids in building community trust in selected pilot sites by implementing strategies addressing implicit bias, procedural justice, and racial reconciliation; the National Forum on Youth Violence Prevention is a network of communities and federal agencies that work together, share information, and build local capacity to prevent and reduce youth violence; and the Violence Reduction Network provides a comprehensive approach to violence reduction that leverages existing resources across DOJ components to reduce crime in some of the country's most violent cities.

By forging state, local, and tribal partnerships among police, prosecutors, judges, victim advocates, health care providers, faith leaders, and others, Office on Violence Against Women (OVW) Services, Training, Officers, Prosecutors (STOP) Formula Grants to States and Grants to Encourage Arrest and Enforcement of Protection Orders help provide victims with the protection and services they need to pursue safe and healthy lives while improving communities' capacity to hold offenders accountable for their crimes. Promoting partnerships between law enforcement and the community is central to the mission of the Office of Community Oriented Policing Services (COPS Office) as crime reduction and community satisfaction are co-dependent entities. To support this effort, the COPS Office manages the COPS Hiring Program to assist state, local, and tribal law enforcement agencies who face economic challenges of keeping their communities safe while maintaining sufficient sworn personnel levels in a changing economic climate. Additionally, the COPS Office continues to partner with grantees to develop innovative publications and resources on a diverse range of topics such as hate crimes, drug market interventions, and identifying hot spots of juvenile offenses.

In addition to supporting national efforts to implement the recommendations outlined in the President's Task Force on 21st Century Policing, the Department, through the COPS Office, released the After-Action Assessment of the Police Response to the August 2014 Demonstrations in Ferguson, Missouri. This assessment, among many other things, highlighted the need for both accountability and transparency as critical components to building and maintaining trust within a community. Following these principles, the Department remains committed to transparency and the Freedom of Information Act process, and is also developing a Fair and Impartial Policing training program for federal law enforcement officers that is based on the COPS Office Fair and Impartial Policing suite of curricula and resources.

The Department's Community Relations Service (CRS) assists in reducing or mitigating conflicts by forging relationships with community leaders, school district officials, and local, city, and state law enforcement and elected officials. CRS works at the grassroots level to assist communities through facilitated dialogue services to help communities open lines of communication among stakeholder groups. CRS also offers consultation services to help communities respond more effectively to conflicts and improve their ability to address underlying issues.

The Department is actively working to improve the collection and analysis of data from local law enforcement agencies. Through the Collaborative Reform and Critical Response Initiative, the COPS Office continues to work with law enforcement agencies to reevaluate the collection and analysis of data in multiple areas such as use of force, traffic stops, and officer involved shootings. The Bureau of Justice Statistics (BJS) and the FBI are working to improve the collection and analysis of crime data through the National Crime Statistics-

Exchange, which aims to improve crime statistics from local police agencies by creating a national system of incident-based crime statistics on crimes known to the police. This system will allow for detailed descriptions of the incidents of violent crimes, including their attributes such as victim-offender relationship, use of a weapon, injury to victims, location and time of day, and other factors. The Arrest-Related Deaths Program is another BJS-FBI collaboration that aims to collect incident-based data on law enforcement use of force that results in serious injury or death, as well as all discharges of weapons at a human subject. This incident-based system would capture data on the characteristics of subjects in the incidents, some attributes of the officers, and the circumstances surrounding the incident. The National Crime Victimization Survey currently obtains data on crimes not reported to the police as well as those reported to the police.

FBI Director Comey has made Uniform Crime Reporting (UCR) Crime Data Modernization one of his top priorities. There is now a dedicated team focused on transitioning law enforcement agencies and UCR state programs that contribute statistical information to the UCR Program to the National Incident-Based Reporting System (NIBRS). The detail available on the incident-level data in NIBRS will enable users to gain better insight into the nature of violent crime, as well as property crimes and crimes against society. The UCR Crime Data Modernization Team is also addressing the lack of information on law enforcement use of force. The FBI UCR Program has proposed the expansion of current data collections to include law enforcement uses of force that result in the death of or serious physical injury to a person, or when the law enforcement officer discharges a firearm at a person.

The Department, through the Civil Rights Division, takes a strategic, efficient, and effective approach to achieving sustainable reform in state and local police jurisdictions by only pursuing cases that involve patterns or practices of severe misconduct, involve new issues of law or policy, respond to exigencies such as rioting or widespread mistrust of law enforcement, and/or can serve as models for other jurisdictions. These cases are very resource intensive, requiring a team of two to four attorneys, an investigator, and paralegal support to complete. To accomplish its complex and difficult enforcement mission to address unconstitutional policing, CRT must: carefully vet a multitude of facts, complaints and allegations to determine when to open an investigation; conduct a fair and thorough investigation, including reviewing thousands of pages of documents, analyzing stop and arrest data, and interviewing police staff and community stakeholders; prepare a publicly-released findings letter when violations are found; engage in sometimes extensive negotiations with jurisdictions to enter a consent decree or settlement agreement that will eliminate the pattern or practice of unconstitutional conduct; monitor implementation of the consent decree or settlement agreement; and, close cases once the pattern or practice has been eliminated.

The Department must carefully assess how to deploy its limited resources to achieve lasting reform. DOJ is limited in the number of new cases that it can bring while fulfilling its obligations in existing cases. CRT works closely with OJP and the COPS Office to ensure that the Department responds to police-community relations issues with the resources and approach most appropriate to the facts of each particular situation.

4. Safeguarding National Security Consistent with Civil Rights and Liberties.

The top priority of the Department is to protect U.S. citizens against acts of terrorism. The Department is also firmly committed to protecting civil rights, civil liberties and promoting transparency. The commitment to protect these rights is evident in the work of the Department's privacy program, which is led by the Department's Chief Privacy and Civil Liberties Officer (CPCLO) and the Office of Privacy and Civil Liberties (OPCL). The CPCLO and OPCL work with privacy officials in each of the Department's components to ensure that privacy and civil liberties protections are incorporated in its important national security work.

DOJ continues to take steps to ensure that it not only focuses on international terrorism but domestic terrorism as well. The Domestic Terrorism Executive Committee (DTEC), was reconstituted late last fiscal year, and now meets on a quarterly basis. The DTEC is co-chaired by a member of the U.S. Attorney community, the NSD, and the FBI, and is designed to ensure collaboration and communication between law enforcement

agencies and components regarding the threat of domestic terrorism. The committee provides a national-level forum for members of the Justice Department, the FBI, and a number of other law enforcement agencies, including several other departments -- Homeland Security, Treasury, Interior, and Agriculture -- to assess and share information about domestic terrorism threats and trends they see from their different vantage points. Within DOJ, the NSD created a new position – counsel for domestic terrorism matters – to assist with its important ongoing work to address and combat domestic terrorism. This domestic terrorism counsel will serve as NSD’s main point of contact for U.S. Attorneys working on domestic terrorism matters, and will not only help ensure that domestic terrorism cases are properly coordinated, but will also play a key role in NSD’s headquarters-level efforts to identify trends to help shape strategy, and to analyze legal gaps or enhancements required to ensure that DOJ can combat these threats. The domestic terrorism counsel will also play an important role with the DTEC by providing its members with insights from cases and trends from around the country

The Department continues to engage in outreach at the local level to foster trust, improve awareness, and educate communities about violence risk factors in order to stop radicalization to violence before it starts. DOJ has been extremely active in community based outreach across a broad range of issues. During the last three years alone, our United States Attorneys have leveraged their unique convening authorities to lead more than 2,500 engagement-related events in their communities.

The Department is working with our partners to build on past successes. DOJ, the Department of Homeland Security, and the National Counterterrorism Center selected three pilot regions to identify promising practices that will inform and inspire community-led efforts throughout the nation. The key to the pilot programs is to broaden the base of community leaders and key stakeholders involved at the local level to help eliminate conditions that lead to alienation and violent extremism, and to empower young people and other vulnerable communities to reject destructive ideologies. The Department is also exploring the possibility of post-conviction programs that might allow for sentencing relief under certain circumstances.

Finally, while the Department is working to protect the nation against terrorism, it is committed to the principles of transparency, oversight, and compliance. The Department appreciates the OIG’s recognition of this commitment and progress with respect to the FBI’s compliance with National Security Letter requirements. In addition, to promote a more transparent government, the Department continues to work with the Office of the Director of National Intelligence and other intelligence community agencies to declassify and make public as much information as possible about certain U.S. Government surveillance programs while protecting sensitive classified intelligence and national security information.

5. Ensuring Effective Oversight of Law Enforcement Programs.

As the nation’s largest law enforcement agency, the Department is responsible for enforcing federal law while maintaining respect for privacy, civil liberties, and civil rights. Appropriate oversight of the Department’s law enforcement components is essential to ensuring the consistent enforcement of federal law. The Department has numerous mechanisms that exist to establish and maintain a consistent approach to law enforcement across all components with a focus on the Department’s strategic and law enforcement priorities. The Attorney General has established guidelines that direct the law enforcement components in the development of policies governing sensitive enforcement methods and tools.

The Department takes very seriously the principle that public service is a public trust, and requires all employees to adhere to certain ethical standards at all times. In response to the January 2015 OIG report, the Department issued more specific guidelines governing off-duty conduct and ethics. The first was a policy issued by Attorney General Holder in April 2015 expressly prohibiting the solicitation, procurement, or acceptance of prostitution, even on personal time and even where such conduct is legal or tolerated in a particular domestic or foreign jurisdiction. Second, an Ethics Handbook for Off-Duty Conduct (Handbook) was developed by the Justice Management Division’s Departmental Ethics Office and issued in August

2015. The Handbook summarizes the principal ethics laws and regulations governing the off-duty conduct of all DOJ employees. Included in the Handbook are rules regarding: misuse of official position, political activities, outside activities (including outside employment), acceptance of gifts, entertainment and favors, conflicts of interest, and special rules for supervisors, special government employees, and attorneys.

In October 2015, the Deputy Attorney General directed all component heads to review and improve their policies and training programs relating to off-duty conduct, with particular focus on ensuring that allegations are properly and promptly investigated and that component charging practices and procedures are tightened and made more effective. This directive included a document entitled *Recommended Practices for Guiding Employee Off-Duty Conduct*, which identified leading practices for components to address the issue of inappropriate off-duty behavior. Further, each component was directed to report to the Departmental Ethics Office its plans to incorporate the guidelines in the component's training. Also in October 2015, the Assistant Attorney General for Administration issued a memorandum for all Department employees regarding off-duty conduct. The memorandum informed employees that they may be disciplined for off-duty conduct if there is a nexus between the offending conduct and the employee's job-related responsibilities. Certain positions, such as law enforcement and attorneys, were warned specifically that their conduct is subject to closer scrutiny with greater potential discipline for off-duty misconduct reflecting on honesty and integrity. Finally, the memorandum noted that marijuana is still a controlled substance under federal law, and all federal employees are required to refrain from the use of illegal drugs even during off duty time. The memorandum was emailed to all Department employees on October 8, 2015, and attached the Ethics Handbook described above. Together, these policies clearly communicated to employees appropriate off duty behavior.

The Department also recognizes that certain law enforcement activities carry potential risks. With regard to the Witness Security (WITSEC) Program, witnesses who are considered for relocation services must be subjected to an intensive vetting process, including a psychological examination, prior to being admitted into the Program. Witnesses are admitted into the Program only after the sponsoring law enforcement agency, the sponsoring United States Attorney, and the United States Marshals Service have provided detailed information and assessments to the CRM's Office of Enforcement Operations (OEO), and after OEO, based on that information and those assessments, has determined that the witness and family members are suitable for the Program, and that the need to admit the witness and family members outweighs the risk to the public and the relocation community. In the OIG review of the WITSEC program, the OIG noted that special consideration should be given to the potential admission of convicted sex offenders and terrorists into the Program. The Department agreed with the OIG's recommendations and has formalized and implemented Program protocols to mitigate the public safety risks posed by such Program participants, in addition to enhancing the sharing of risk information with other law enforcement officers. The Department believes that these changes were necessary, will provide additional security to the public, and will ensure greater internal oversight.

Regarding the use of confidential sources, the Drug Enforcement Administration (DEA) and CRM have undertaken a comprehensive review of DEA's confidential source policy. The policy is being revised to ensure that it is fully consistent with the *Attorney General's Guidelines Regarding the Use of Confidential Sources*. The revised policy will address the concerns raised by the OIG in its July 2015 Report, and it will ensure that the risks of using a confidential source are fully evaluated and considered before he or she is used and that adequate supervision is provided whenever a confidential source provides assistance. The revised policy is currently being reviewed by senior DOJ and DEA leadership. The FBI's use of Confidential Human Sources is governed by the *Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources* and by FBI policy, which specifically address the oversight required to effectively manage the risk that an FBI confidential source will take advantage of his/her status and break the law. The guidelines seek to manage this risk from the beginning of the FBI's operational relationship with the confidential source by requiring that, unless specifically authorized, the source is informed not to engage in criminal activity because he/she has no immunity from prosecution for any unauthorized criminal activity. This admonishment must be provided by at least one FBI agent with another government official present as a witness, and sets a clear

expectation that the source will not be protected by the FBI if he/she engages in unauthorized criminal activity.

The Department appreciates the complexities, nuance, and risks associated with international law enforcement activities. DEA in particular has long followed a systematic, comprehensive operational planning and approval process that incorporates risk management assessments and guidance from senior DEA and DOJ leaders. DEA also remains mindful of evolving risk assessment requirements within DOJ, as well as developing best practices among U.S. interagency partners. Accordingly, the Department works continually to refine its operational planning practices, and to enhance its risk and consequence management efforts.

Through outreach, training, conferences, and active participation in various state and judicial venues, the Department is working toward timelier reporting of full and accurate criminal history records via the National Instant Criminal Background Check System (NICS). DOJ is auditing NICS to evaluate its effectiveness; focusing on how the FBI refers NICS purchase denials to the ATF, the ATF's review of those referrals, and whether prosecutions result from this process. The Department also supports states in the modernization of state records management systems so that final dispositions can be received electronically and is surging resources to reduce the number of delayed NICS transactions and allow executive management to better assess resource allocation. The FBI plans to deploy its "New NICS" in January 2016, which will provide processing efficiencies, timely system updates, and improved data sharing. In addition, the Department is evaluating options to search additional FBI databases that may prove beneficial in resolving delayed transactions.

Because the integrity of the Department is dependent upon the conduct of its individual employees, DOJ regards allegations of employee sexual harassment or misconduct in its law enforcement components very seriously. As the OIG stated, the FBI's offense table clearly addresses allegations of sexual misconduct and sexual harassment. The FBI Office of Professional Responsibility takes great care to ensure that the misconduct results in an appropriate and consistent disciplinary response. In response to the OIG report, ATF updated its table of penalties to include new offense categories for solicitation of prostitutes and inappropriate workplace relationships, as well as a category for sexual misconduct, and also instituted a mandatory Standards of Conduct training. The U.S. Marshals Service (USMS) supervisors and managers are required to report all allegations of sexual misconduct and sexual harassment to headquarters, and all employees are required read and acknowledge their understanding of the Code of Professional Responsibility. Following the OIG report, DEA reviewed its standards of conduct and disciplinary policies, examined and evaluated the offense categories specifically designed to address sexual misconduct and sexual harassment, and revised the table of offenses to coincide with other law enforcement components. As of October 2015, DEA has completed all actions required by the OIG.

Asset forfeiture is an important tool in law enforcement, and as such the Department ensures that its asset seizure programs and activities are effectively monitored, directed, and supervised. Following the Attorney General's order in January 2015, the Department strengthened federal oversight in state and local asset seizures in which the DOJ agencies were involved. A pivotal aspect of the Attorney General's order was determining whether there was federal law enforcement oversight and participation at the time of the seizure by state and local law enforcement officers. In response, DOJ promulgated additional guidance on February 10, 2015, in Policy Directive 15-2, which provided factors to consider when deciding whether a seizure qualified as a task force or joint investigation seizure and required a two-step approval process to ensure that the forfeiture was permissible under the Attorney General's order. The FBI has conducted field training at various field offices and a national Asset Forfeiture training to various Chief Division Counsels, Assistant Division Counsels, Agents, and other FBI employees to ensure compliance with the new policy, while DEA effectively implements training, policy and operational requirements for law enforcement personnel regarding interdiction operations at mass transportation facilities worldwide.

Regarding the Department's use of Unmanned Aircraft Systems in law enforcement operations, on June 29, 2015 the FBI and the Federal Aviation Administration (FAA) signed a memorandum of

understanding that expands the locations and times that the FBI can operate its drones without first requesting written FAA permission.

6. Promoting Public Confidence by Ensuring Ethical Conduct throughout the Department.

As noted above, the Department takes very seriously the principle that public service is a public trust, and requires all employees to adhere to certain ethical standards at all times. While it is impossible for any organization as large and complex as the Department to maintain a perfect record, DOJ strives to vigilantly maintain the integrity of its employees in order to ensure public confidence in the administration of justice.

The Department has made significant improvements in the hiring process for full time employees, contractors and interns and has closed the previous weakness identified in the OIG report related to INTERPOL Washington. INTERPOL Washington has restructured its administrative management team by reassigning the duties of the previous Executive Officer position to newly created Chief Financial Officer and Administrative Officer positions. These new senior management positions now share oversight responsibility over all administrative, human resources, and financial business processes. All INTERPOL Washington supervisors and participants in the hiring process are required to complete mandatory Human Resource and Hiring training courses, and every selected new employee, contractor, and intern must complete and sign a DOJ/Justice management Division (JMD) Disclosure Form to disclose the names of any family members who are currently employed by the Department. The disclosure form, in addition to the independent review conducted by JMD Human Resources, provides sufficient internal and external controls to prevent future nepotism or favoritism in INTERPOL Washington's hiring practices. Regarding the OIG report on a case of USMS favoritism in hiring, JMD is currently reviewing USMS hiring case files and policies. The USMS has provided JMD with requested available hiring cases dating back to 2010 as well as policies and standard operating procedures. The review is ongoing and the USMS will continue to provide requested information and records.

The Department agrees that it must ensure that its employees safeguard sensitive information they encounter in the course of their duties and has taken multiple actions to mitigate this type of threat. The FBI established the Insider Threat Center (InTC) in FY 2015 to centralize coordination of the Insider Threat Program, including issues related to the safeguarding of sensitive information. The FBI developed a new, all personnel training module that covers the handling and safeguarding of sensitive information among other insider threat topics. Additionally, the InTC is developing a referral system to automate a risk-based review of FBI personnel that exhibit behaviors consistent with those associated with insider threats. FBI has revised its policy on handling drug evidence in response to the lack of controls identified by OIG as part of the Lowry investigation. The newly published Field Evidence Management Policy Guide, effective in April of 2015, adds additional restrictions on drug handling and transporting including additional requirements for supervisor approval. DEA has implemented additional controls to help detect any potential fraud, including a bi-weekly reconciliation of the list of travel card holders obtained directly from the bank with DEA's employment records, and review of that reconciliation by the Financial Integrity Section. In addition to ensuring that travel cards are active only for employees and task force officers on board and that this process is segregated and performed independently, routine delinquency monitoring has also been segregated and is performed completely independent. DEA is also pursuing preventative controls, including having the bank run credit worthiness checks on each application submitted and requiring multi-person approvals on credit card applications. DEA has established ethical guidelines for its employees that form the basis for the Standards of Conduct issued and acknowledged annually by every DEA employee. Supervisors and employees alike are required to report violations of the Standards of Conduct to their respective supervisors or the Office of Professional Responsibility; failure to report such allegations may result in serious sanctions for the subject employee. The Office of Professional Responsibility refers every allegation of misconduct to both the DOJ OIG and to the DEA Office of Security Programs for review.

The Department recognizes the important role played by whistleblowers. To help educate employees about their rights as whistleblowers, in April 2014, the Deputy Attorney General sent a memo to all employees that

discussed the importance of reporting waste, fraud, and abuse and provided a link to a training video on whistleblowers' rights created by the OIG. The Department has also taken a number of steps to improve the process for FBI employees who report complaints. Specifically, Department has provided additional resources to the Office of Attorney Recruitment and Management, ensured access to alternative dispute resolution, and the FBI has created a new training program for all FBI employees. Additionally, the Department has committed to drafting new regulations to update its whistleblower protection procedures for FBI employees, including proposing to expand the list of officials to whom a protected disclosure may be made.

In response to the OIG's statement that on occasion they were not provided timely access to certain records, the Department has repeatedly stated its commitment to ensuring that the OIG has access to the information it needs to perform its oversight mission effectively. In every instance where the OIG has sought access to legally-restricted material – such as grand jury material protected by Federal Rule of Criminal Procedure 6(e), Title III wiretap information, or materials protected by the Fair Credit Reporting Act – from the Department, the Attorney General or the Deputy Attorney General has ensured that the OIG obtained the requested material. In keeping with our commitment, the Department has been working to draft a legislative proposal that would guarantee that its OIG has access to the information it needs to conduct its investigations and reviews, including information protected from disclosure by statutes such as the Federal Wiretap Act, Rule 6(e) of the Federal Rules of Criminal Procedure, and section 626 of the Fair Credit Reporting Act (FCRA). On November 3, 2015, the Department provided to Congress draft legislation to ensure that OIG receives the documents it needs to complete its reviews. We look forward to working with OIG and Congress to address this important issue.

The Department disagrees with the OIG's stance on the jurisdiction of the Department's Office of Professional Responsibility (OPR). OPR was created to investigate allegations of misconduct against Department attorneys that relate to their authority to litigate, investigate, or provide legal advice, and OPR has acquired considerable expertise in the state ethical and professional rules of conduct that governs the practice of law by Department attorneys. The OIG report contains no criticism of OPR's work, the thoroughness of its investigations, or the soundness of its findings. OPR acts independently and without interference from Department senior leadership. The Department is not aware of any reason why this model should be changed. Where appropriate, OPR has investigated senior Department leadership at the highest levels and issued misconduct findings against Department attorneys when evidence supported such findings. Should the OIG want to assume an investigation that falls within the jurisdiction of OPR, a formal mechanism exists for the OIG to make such request.

Regarding transparency, notwithstanding Privacy Act limitations, OPR annually reports statistical information on the complaints it receives and the number of inquiries and investigations it accepts and resolves. This includes the sources of complaints and allegations; the categories of allegations made and resolved; and whether closed investigations resulted in findings of professional misconduct, poor judgment, or mistake. OPR's annual reports not only include summaries of representative inquiries handled by OPR during the year but also include summaries of nearly every investigation OPR closed during the fiscal year. In addition, OPR regularly provides complainants detailed information concerning the resolution of their complaint, and the Department refers to bar disciplinary authorities any findings of professional misconduct that implicate bar rules.

The Department takes seriously the need to take effective disciplinary action against employees who have engaged in misconduct, especially attorneys who have committed professional misconduct. That is just one reason why the Department created the Professional Misconduct Review Unit (PMRU). In announcing the creation of the PMRU on January 14, 2011, the Attorney General noted that Department attorneys are dedicated to the cause of justice, and demonstrate on a daily basis their commitment to the highest ethical standards. The PMRU is dedicated exclusively to the fair, but expeditious resolution of disciplinary matters arising out of findings of professional misconduct by OPR. This singular focus has allowed the PMRU to increase the timeliness of resolutions and to ensure the consistent and equitable treatment of similarly-situated

employees. Moreover, the PMRU has provided Department attorneys with a fair and transparent opportunity to respond to OPR's findings of professional misconduct and any disciplinary actions arising from such findings. The PMRU established a record of efficiently and effectively handling the matters referred to it and its operations are fully consistent with the requirements of federal law and regulations. To build on the PMRU's success, the Deputy Attorney General issued a memorandum on January 30, 2015, that extends the PMRU's disciplinary and bar referral authority to attorneys who work in nearly all Department of Justice components. This expansion ensured timely and consistent resolutions of misconduct allegations throughout the Department.

7. Effectively Implementing Performance-Based Management.

The Department is committed to the development of results-oriented performance measurement and has processes in place to monitor and improve its measures. As stated in the OIG's Report, establishing performance measures directly linking to outcomes is a challenge for many of the Department's programs given that the programmatic outcomes frequently are not easily quantified nor entirely within the control of the program.

The Department recently published new FY 2016-2017 Priority Goals through performance.gov, reflecting the Attorney General's top priorities through results-oriented measures related to national security, cybercrime, strengthening relationships with communities, vulnerable people, and fraud and public corruption. As part of the Quarterly Status Review process, the Department reviews and monitors component performance data, along with budget execution and financial information. Additionally, per the Strategic Objective Review, the Department conducts an annual assessment on the progress toward achieving the strategic objectives described in the DOJ Strategic Plan. The Strategic Objective Review includes an analysis of both the quality and the progress of performance measures, and often results in planned next steps to either improve existing measures or to create new measures to better show the results of DOJ programs and activities.

The Department agrees that better recordkeeping is important to help assess the results of its initiatives. In regards to Smart on Crime, the Department will continue to assess, clarify, and provide greater context concerning the 16 indicators to make them more accessible and understandable. However, it is worth noting that these indicators were not initially designed for the purpose of incentivizing prosecutorial conduct by setting measurable targets or goals. The Department must be careful in the way it measures performance, mindful that in some instances, requiring certain results-oriented outcomes could potentially violate professional standards of ethical conduct or lead to unintended and possibly adverse consequences. In particular, DOJ is reluctant to set goals or targets for discretionary prosecutorial activity, such as charging or declining cases or initiating diversion programs. Nevertheless, current data has allowed the Department to make some helpful preliminary assessments of Smart on Crime: (1) drug defendants are being charged with a crime carrying a mandatory minimum sentence twenty percent less frequently than before the Smart on Crime Initiative; (2) fewer defendants were charged with federal crimes in 2015, as compared to prior years; and (3) overall sentences in drug cases have been reduced post-Smart on Crime.

To address data on recidivism, BOP has developed an evaluation plan that includes all national reentry programs. BOP has completed the research methodology for the Residential Sex Offender Treatment Program evaluation, which will evaluate rates of recidivism as measured by whether a treatment subject or comparison subject was arrested after release from prison for a sexual offense or for another offense. Comparison subjects, chosen from a pool of untreated sex offenders considered for residential treatment, were selected to approximate the characteristics of treatment subjects. The first of the periodic examinations of recidivism are near completion, with more to come over time.

Regarding the Department's debt collection program, the Consolidated Debt Collection System (CDCS) was not designed to be a case tracking system, performance management system, or business management tool for EOUSA and the Financial Litigation Units (FLUs) in the various USAOs. Rather, the CDCS is a debt

collection Information Technology system that assists FLUs and other applicable personnel in establishing debts, corresponding with debtors through the generation and mailing of documents, recording account balances and the accrual of interest, recording payments received from debtors, and performing other financial and administrative tasks associated with the collection of debts. The Department initiated work on an analytics capability in 2013 to better use information stored in CDCS to assist EOUSA with improving debt collection. Since that time, several reporting dashboards have been created that allow EOUSA to compare debt collection performance between entities and measure debt collection effectiveness. The Debt Collection Management Staff is experimenting with estimating debt collectability and working to add new variables that will improve accuracy and reliability of this information.

The Department of Justice *Human Capital Strategic Plan for 2015-2018* includes the goal of Strengthening the DOJ Workforce. To operationalize the strategic plan, the Department has annual Strategic Human Capital Objectives that include initiatives such as increasing the number of new hires by renewing focus on the Pathways program, establishing a DOJ Recent Graduates program, and utilizing all available authorities to hire the highest quality workforce in the most efficient manner possible while upholding the Merit Systems Principles and avoiding Prohibited Personnel Practices. These objectives demonstrate that the Department recognizes the need to plan for the future DOJ workforce, and is taking action to provide the necessary infrastructure for hiring and developing new talent.

The Department is also actively participating in the government-wide Executive Steering Committee on Closing Skill Gaps in Mission Critical Occupations (MCOs). The Committee has identified government-wide and agency-specific mission critical occupations, and is working to identify high-risk MCOs and develop strategies, set targets, monitor progress, and evaluate results in mitigating those risks. The Department recently established and filled a position dedicated to strategic human capital management. In part, this position is responsible for providing data and supporting workforce planning initiatives for DOJ MCOs. DOJ is enhancing the utility of HRStat data-driven reviews by involving stakeholders from outside the Human Capital community to enrich their understanding of Human Capital strategic goals and objectives. As part of the Department's quarterly HRStat review, JMD Human Resources and DOJ components will report progress in closing any skill gaps for MCOs, and will reach out to stakeholders from those occupational communities to share data regarding the health and vitality of their occupations. These actions demonstrate that the Department is fully engaged in strategic workforce planning for DOJ's current and future workforce.

8. Protecting Taxpayer Funds from Mismanagement and Misuse.

The Department concurs with the OIG that there are numerous opportunities for improved efficiency to save taxpayer dollars. To that end, the Department takes proactive measures to continually assess areas in which it might create savings and improved monitoring of funds within the Department's control. DOJ takes very seriously its responsibility to protect taxpayer dollars, and has taken numerous steps in recent years to ensure that Department resources are being managed efficiently and effectively.

Funds Spent within the Department

The OIG stated in its report that the FBI, Criminal Division, National Security Division (NSD) and Executive Office for U.S. Attorneys and U.S. Attorney's Offices have made extensive use of Temporary Duty (TDY) but did not adequately track extended TDY. Travel and extended travel are often required to accomplish the mission of the Department's components. JMD Finance has drafted and will soon finalize and issue Department-wide travel policy that addresses the concerns made by the OIG. These new travel policies will allow for better tracking of expenses and extended travel provisions and will allow for stronger oversight and control of the Division's resources. In anticipation of the new travel policy, components have instituted controls and procedures to manage travel and control costs. FBI employees on TDYs, including joint duty assignments, are tracked in the FBI's human resources system, HRSource. Both CRM and EOUSA put into place new processes to report and track extended TDY. EOUSA management has also sought a written opinion from the Internal Revenue Service on the taxability of housing provided to detailees at the National

Advocacy Center. Finally, NSD has made significant changes to its extended TDY record-keeping practices to ensure accuracy and consistency.

The OIG found that the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) spent approximately \$600,000 on Unmanned Aircraft Systems (UAS) vehicles, commonly referred to as drones, but never flew them operationally. A week after ATF suspended its UAS program and disposed of the drones, another ATF staff spent approximately \$15,000 for five commercial drones. ATF issued a policy requiring the purchase of UAS to be approved by the Deputy Assistant Director for Programs and coordinated through the Special Operations Division (SOD). Further, the policy requires SOD to conduct a needs analysis prior to the purchase of UAS. OIG considered these actions sufficient and closed the recommendation.

EOUSA agrees with the OIG that sufficient resources should be allocated to the debt collection function, however in balancing competing resource demands, the collectability of outstanding debt must also be considered in determining the appropriate staffing levels. EOUSA recognizes the potential benefits of more effective asset recovery collaboration within the U.S. Attorneys' offices and has commenced a comprehensive review to identify practices and strategies that would enhance its debt collection efforts. EOUSA is committed to developing and implementing new and innovative debt collection policies, practices, and resources that will take full advantage of technological advances and leverage existing resources to fulfill its debt collection mission.

Funds Spent via Contracts and Grants

The Office of Justice Programs (OJP) agrees that proper oversight of grant funds and administering those funds in the most fair and transparent way possible is critical; as such, grant oversight is unequivocally one of OJP's highest priorities. OJP integrates programmatic, financial, and administrative oversight throughout the grant lifecycle. OJP consistently exceeds its statutory requirement to conduct comprehensive monitoring of not less than 10 percent of total award dollars. In FY 2015, OJP completed in-depth programmatic monitoring of nearly 800 grants totaling \$1.1 billion, two times the amount required by law. In-depth programmatic monitoring (on-site or remote) is an extensive review of the grantee's activities. OJP also conducts annual programmatic desk reviews on each of its nearly 7,000 active grants. Annual desk reviews ensure compliance with programmatic and administrative requirements and assess progress towards the program goals and objectives as forth in the award.

For FY 2015, OJP's Office of the Chief Financial Officer (OCFO) monitored and reviewed approximately \$1.4 billion (more than 10 percent) of active grant awards. This included on-site financial monitoring of 482 grants totaling \$951 million, and 433 desk reviews totaling more than \$461 million. As a result, OCFO identified almost \$19 million in questioned costs and is pursuing corrective action with the grantees. In FY 2015, 505 grantees successfully completed OJP's on-line grants financial management training, 169 grantees attended OJP's in-person financial training seminars, and an additional 601 grantees attended special ad hoc training sessions customized to their needs.

OJP's Office of Audit, Assessment, and Management manages the DOJ-wide high-risk grantee designation process. DOJ's high-risk process provides for increased oversight and monitoring, as well as additional special conditions that restrict use of existing and/or new grant funds without prior formal approval. The COPS Office is also required by statute to monitor 10 percent of its active award portfolio each year and they use many of the same procedures as OJP, including a risk-based, data-driven approach to their oversight and monitoring. The COPS Office reports consistently accomplishing this goal each year.

OJP recognizes the increased risk presented with the additional funding appropriated under the Crime Victims Fund (CVF). In FY 2015, OJP authorized the hiring of additional positions to conduct financial monitoring and oversight activities. In addition to its standard oversight and management efforts, OJP and the Office for Victims of Crime (OVC) are taking the following steps to ensure sound stewardship of funding under the CVF, to include: increasing staff resources at the program office level as well as within OCFO to oversee and

monitor the funds; incorporating additional risk criteria to its risk assessment process in FY 2016 to increase the monitoring priority of these awards; and preparing quarterly risk indicator reports to proactively identify and resolve potential issues. As part of these efforts, OCFO and OVC is enhancing its monitoring of Victim Compensation and Victim Assistance grants through increased on-site monitoring and improvements to performance measurement activities, including requiring more frequent reporting of measures within a new performance management system.

OJP is working with OIG to resolve outstanding issues regarding jail construction grants to the Navajo Nation and is working with OIG to resolve outstanding issues. OJP, OVW, and COPS Office are developing training videos for tribes on the DOJ grant award process and how to develop and implement sound grant management practices. Elements of the series include an overview of the DOJ grants lifecycle, as well as grant fraud, waste, and abuse. The Department anticipates the videos will be released in early 2016.

The OIG report cited concerns with OJP's oversight of grant awards. In FY 2015, DOJ worked with 125 grantees designated as high-risk, including the Puerto Rico Department of Justice (PRDOJ). Based on OIG's findings for PRDOJ, coupled with the Commonwealth's financial climate, OJP took immediate action to protect the federal funds awarded to Puerto Rico, including designating the entire Commonwealth as a DOJ high-risk grantee, imposing immediate holds on Puerto Rico's access to existing and new grant awards, and adding new award special conditions to Puerto Rico's remaining open grants, which permits the drawdown of funds by formal request and approval only. DOJ leadership is actively involved in the White House interagency task force on Puerto Rico, which was established to address issues with Puerto Rico. OJP provides frequent updates to DOJ leadership on the status of Puerto Rico's grants, including programmatic and financial data.



Corrective Action Plan

FMFIA SECTION 2 – PROGRAMMATIC MATERIAL WEAKNESS – PRISON CROWDING

U.S. DEPARTMENT OF JUSTICE Corrective Action Plan Issue and Milestone Schedule		Report Date September 30, 2015															
Issue Title Prison Crowding	Issue ID 06BOP001	Component Name Bureau of Prisons															
Issue Category <table style="width: 100%; border: none;"> <tr> <td style="width: 30%;">FMFIA, Section 2</td> <td style="width: 10%; text-align: center;"><input type="checkbox"/></td> <td style="width: 30%;">Reportable Condition</td> <td style="width: 10%; text-align: center;"><input checked="" type="checkbox"/></td> <td style="width: 19%;">Material Weakness</td> </tr> <tr> <td>FMFIA, Section 4</td> <td style="text-align: center;"><input type="checkbox"/></td> <td>Non-conformance</td> <td></td> <td></td> </tr> <tr> <td>OMB A-123, Appendix A</td> <td style="text-align: center;"><input type="checkbox"/></td> <td>Reportable Condition</td> <td style="text-align: center;"><input type="checkbox"/></td> <td>Material Weakness</td> </tr> </table>			FMFIA, Section 2	<input type="checkbox"/>	Reportable Condition	<input checked="" type="checkbox"/>	Material Weakness	FMFIA, Section 4	<input type="checkbox"/>	Non-conformance			OMB A-123, Appendix A	<input type="checkbox"/>	Reportable Condition	<input type="checkbox"/>	Material Weakness
FMFIA, Section 2	<input type="checkbox"/>	Reportable Condition	<input checked="" type="checkbox"/>	Material Weakness													
FMFIA, Section 4	<input type="checkbox"/>	Non-conformance															
OMB A-123, Appendix A	<input type="checkbox"/>	Reportable Condition	<input type="checkbox"/>	Material Weakness													
Issue Category – SAT Concurrence or Recategorization Concur																	
Issue Description <p>As of September 30, 2015, the inmate population housed in BOP operated institutions exceeded the rated housing capacity by 23 percent, down from an overcapacity rate of 30 percent as of the end of FY 2014. The impact of the Department’s Smart on Crime initiative, legislative changes, and Clemency have all contributed to reducing the inmate population; nonetheless, the BOP continues to experience dangerously high levels of crowding particularly at higher-security institutions.</p> <p>Crowding presents critical safety challenges for both staff and inmates. In addition, crowding has a negative impact on the ability of the BOP to promptly provide inmate treatment and training programs that promote effective re-entry and reduce recidivism. For example, because of years of high overcapacity rates and understaffing, a significant number of inmates are on waiting lists for most inmate programs, to include the GED program with approximately 16,000 inmates on the waiting list. While every effort is being made by the BOP to address the backlog, it will take several years due to limited classroom size and teaching staff, as well as the rising costs associated with offering the program in multiple languages and regularly upgrading computer equipment and training content to ensure the program is aligned with community standards. The FY 2015 budget for the BOP was essentially flat from the FY 2014 level. The proposed FY 2016 budget takes into account the declining inmate population but includes investments in additional staffing and inmate treatment and training programs that promote effective re-entry and reduce recidivism.</p> <p>To address this material weakness, the BOP will continue implementing its Long Range Capacity Plan, making enhancements and modifications to the plan, as needed, commensurate with funding received through enacted budgets.¹ The BOP’s formal Corrective Action Plan includes utilizing contract facilities; expanding existing institutions; and acquiring, constructing, and activating new institutions as funding permits. The BOP will continue to validate progress on construction projects at new and existing facilities through on-site inspections or by reviewing monthly construction progress reports.</p> <p>This material weakness was first reported in 2006. Remediation of the weakness through increasing prison capacity is primarily dependent on funding. Other correctional reforms and alternatives will require policy and/or statutory changes. Other initiatives notwithstanding, if the acquisition, expansion, construction, and activation plans detailed in the BOP’s Long Range Capacity Plan are funded as proposed, the overcapacity rates for FYs 2016 and 2017 are projected to be 12 percent and 11 percent, respectively.</p> <p>The Department’s corrective action efforts are not limited to the BOP alone. The Department continues to consider and implement an array of crime prevention, sentencing, and corrections management improvements that focus on accountability and rehabilitation, while protecting public safety. The Department recognizes that the BOP’s capacity management efforts must be teamed with targeted programs that are proven to promote effective re-entry and reduce recidivism. The BOP will continue to work with the Department on these programs.</p>																	

¹ The BOP’s Long Range Capacity Plan relies on multiple approaches to house the federal inmate population, such as contracting with the private sector and state and local facilities for certain groups of low-security inmates; expanding existing institutions where infrastructure permits, programmatically appropriate, and cost effective to do so; and acquiring, constructing, and activating new facilities as funding permits.

Business Process Area (N/A for Section 2 and Section 4 issues)			
Not Applicable			
Date First Identified	Original Target Completion Date	Current Target Completion Date	Actual Completion Date
2006	09/30/2012	Dependent on funding	
Issue Identified By		Source Document Title	
Bureau of Prisons		BOP Population Projections	
Description of Remediation			
Increase the number of federal inmate beds to keep pace with the projected inmate population. Efforts to reach this goal include expanding existing institutions, acquiring surplus properties for conversion to correctional facilities, constructing new institutions, utilizing contract facilities, and exploring alternative options of confinement for appropriate cases.			
Milestones	Original Target Date	Current Target Date	Actual Completion Date
1. As of September 30, 2006, the inmate population in BOP owned and operated institutions reached 162,514 and was housed in a capacity of 119,510, resulting in an over-crowding rate of 36 percent.	09/30/2006		09/30/2006
2. As of September 30, 2007, the inmate population in BOP owned and operated institutions reached 167,323 and was housed in a capacity of 122,189, resulting in an over-crowding rate of 37 percent, an increase of 1 percent for the year.	09/30/2007		09/30/2007
3. As of September 30, 2008, the inmate population in BOP owned and operated institutions reached 165,964 and was housed in a capacity of 122,366, resulting in an over-crowding rate of 36 percent, a decrease of 1 percent for the year.	09/30/2008		09/30/2008
4. As of September 30, 2009, the inmate population in BOP owned and operated institutions reached 172,423 and was housed in a capacity of 125,778, resulting in an over-crowding rate of 37 percent, an increase of 1 percent for the year.	09/30/2009		09/30/2009
5. As of September 30, 2010, the inmate population in BOP owned and operated institutions reached 173,289 and was housed in a capacity of 126,713, resulting in an over-crowding rate of 37 percent, the same rate as at the end of the previous year.	09/30/2010		09/30/2010
6. As of September 30, 2011, the inmate population in BOP owned and operated institutions reached 177,934 and was housed in a capacity of 127,795, resulting in an over-crowding rate of 39 percent, an increase of 2 percent for the year.	09/30/2011		09/30/2011
7. As of September 30, 2012, the inmate population in BOP owned and operated institutions reached 177,556 and was housed in a capacity of 128,359, resulting in an over-crowding rate of 38 percent, a decrease of 1 percent for the year.	09/30/2012		09/30/2012
8. As of September 30, 2013, the inmate population in BOP owned and operated institutions reached 176,849 and was housed in a capacity of 129,726, resulting in an over-crowding rate of 36 percent, a decrease of 2 percent for the year.	09/30/2013		09/30/2013
9. As of September 30, 2014, the inmate population in BOP owned and operated institutions reached 172,742, and was housed in a capacity of 132,803, resulting in an over-crowding rate of 30 percent, a decrease of 6 percent for the year.	09/30/2014		09/30/2014
10. As of September 30, 2015, the inmate population in BOP owned and operated institutions reached 165,164 and was housed in a capacity of 134,470, resulting in an overcapacity rate of 23 percent, a decrease of 7 percent for the year.	09/30/2015		09/30/2015

Milestones	Original Target Date	Current Target Date	Actual Completion Date
11. Planning estimates call for a rated capacity of 135,174 to be reached by the end of FY 2016. The over-crowding rate is projected to be 13 percent at that time, a decrease of 10 percent for the year.	09/30/2016		
12. Planning estimates call for a rated capacity of 136,250 to be reached by the end of FY 2017. The overcapacity rate is projected to be 11 percent at that time, a decrease of 2 percent for the year.	09/30/2017		
<p>Reason for Not Meeting Original Target Completion Date Funding received through enacted budgets through FY 2011 did not keep pace with the increases in the federal inmate population. Although decreases in the population since then have reduced the overcapacity rate, further reductions in the rate are largely dependent on funding received being consistent with the funding needs identified in the BOP Long Range Capacity Plan.</p>			
<p>Status of Funding Available to Achieve Corrective Action FY 2016 funding is unknown at this point because the FY 2016 budget has not been enacted. The Department of Justice's proposed FY 2017 budget for BOP is under review at the Office of Management and Budget.</p>			
<p>Planned Measures to Prevent Recurrence The BOP will continue to structure budget requests to address capacity needs in the most cost effective manner possible.</p>			
<p>Validation Indicator Results are measured as a new institution or expansion project is activated and resulting increases in rated capacity are established. A corresponding decrease in the over-crowding rate will be a tangible measurement of the results. Progress on construction projects at new and existing facilities will be validated via on-site inspections of each facility or by review of monthly construction progress reports.</p>			
<p>Organizations Responsible for Corrective Action BOP Administration Division and Program Review Division</p>			

This page intentionally left blank.

Undisbursed Balances in Expired Grant Accounts

Section 536 of the Commerce, Justice, Science, and Related Agencies Appropriations Act, 2012 (Act) of the Consolidated Appropriations Act, 2010 (Pub. Law 112-55) requires certain departments, agencies, and instrumentalities of the United States Government receiving appropriations under the Act to track undisbursed balances in expired grant accounts for FY 2015.

Undisbursed balances in expired grant accounts include budget authority that is no longer available for new obligations but is still available for disbursement. According to Section 20.4(c) of OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, the expired phase "lasts five years after the last unexpired year unless the expiration period has been lengthened by legislation. Specifically, you may not incur new obligations against expired budget authority, but you may liquidate existing obligations by making disbursements." For FY 2015, the below information is required to be reported in the Agency Financial Reports and annual performance plans/budgets with regard to undisbursed balances in expired grant accounts: 1) details on future action the department, agency, or instrumentality will take to resolve undisbursed balances in expired grant accounts; 2) the method that the department, agency, or instrumentality uses to track undisbursed balances in expired grant accounts; 3) identification of undisbursed balances in expired grant accounts that may be returned to the Treasury of the United States; 4) in the preceding three fiscal years, details on the total number of expired grant accounts with undisbursed balances (on the first day of each fiscal year) for the department, agency, or instrumentality and the total finances that have not been obligated to a specific project remaining in the accounts.

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

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

COPS closely monitors the financial activity of all its grantees. This includes requiring all grant recipients to report the financial expenditures for all COPS awards on a quarterly basis. COPS has a dedicated group of Grant Program Specialists and Staff Accountants that offer grantees real-time technical assistance on implementation of their grant(s).

Due to the additional reporting requirements and transparency associated with American Recovery and Reinvestment Act of 2009 (ARRA) grant recipients, COPS implemented additional efforts to monitor COPS Hiring Recovery Program (CHRP) grantees. CHRP grantees were encouraged to complete an online grants management training, which included a training track focused on financial reporting and disbursement of funds. CHRP grantees were also notified in 2012 of the September 30, 2015 lapse (5 years after the last unexpired year for ARRA) of undisbursed balances on CHRP awards and reminded that all grant program requirements should be completed by that time and all expensed funds should be disbursed. Finally, in November 2010, COPS began conducting quarterly outreach efforts to CHRP grantees that appear to have discrepancies in the financial and/or programmatic reporting on their awards.

The COPS Grants Administration Division and the COPS Finance Business Unit collaborated to create a notification system to alert grantees that still have available funds at 120 days before the grant end date. The alert encouraged these grantees to review their grant program requirements and take advantage of the impending arrival of an extension letter, as needed. Grant Program Specialists contact grantees several times before the grant end date so that Post-Close requests for extensions can be averted. After reaching the grant end date, COPS Finance staff compares the expenditures listed on the final Financial Status Report with the Financial Management Information System 2 (FMIS2) balance of funds that have previously been disbursed. If there is an eligible disbursement available, the grantee will receive a notice approximately every 30 days instructing them to draw down the eligible balance before the 90 day grace period ends. All CHRP grants

were included in this process leading up to the ARRA funds expiration deadline. The COPS Office finished the 2015 fiscal year with a \$0 balance of CHRP (ARRA funds) grants. COPS management worked with the Justice Management Division (JMD), Office of Management and Budget (OMB), and the Office of the Vice President (OVP) to ensure that ARRA funds were being disbursed and outlaid in a timely manner.

All OJP discretionary/categorical and block/formula grantees are required to submit a financial report quarterly. Grantees have 90 days after the end date of the award to drawdown funds and close out the award. If the payments to the grantee are less than the amount of the grant expenditures, then the grantee is given the opportunity to draw down these funds. OJP Customer Service Outreach staff calls the grantee to ask them to draw down their funds. The first notice will commence on the same day as the phone call to the grantee. If the grantee has not drawn down their available funds after 14 calendar days, a second contact is made by the Customer Service Outreach staff and a second notice is sent. If there is no action by the grantee, a third notice is sent to the grantee informing them that OJP will de-obligate the funds from their grant. If the grantee has not retrieved their funds after 14 additional calendar days, the funds are de-obligated. After deobligation, the grantee will receive a Grant Adjustment Notice (GAN) in the mail informing them that the funds have been de-obligated and are no longer available and the grant is closed.

OVW closely monitors the financial activity of all its grantees. All grant recipients are required to report their financial expenditures for OVW awards on a quarterly basis and their project performance activities on a semi-annual or annual basis. Although Section 1512 reporting was terminated in January 2014, until that time, ARRA grantees were required to submit special Section 1512 reports on a quarterly basis that included project and financial information. OVW reviewed 100 percent of these reports for each reporting period and contacted the grantees regarding any concerns or questions. OVW Grant Program Specialists and Financial Analysts offered ARRA grantees technical assistance with implementing any aspect of their grant, including trainings, outreach, site visits and monitoring. The OVW management received and reviewed frequent reports on ARRA grant activity, including obligation and outlay data, and OVW management worked with JMD, OMB, OVP, and the OIG to ensure that ARRA funds were being disbursed and outlaid timely. The OVW ARRA Supplemental Appropriation was cancelled on September 30, 2015, and unobligated balances were returned to Treasury.

2. Method used to track undisbursed balances in expired grant accounts:

COPS utilizes FMIS2 data and data from OJP's Grant Payment Request System (GPRS) to track CHRP undisbursed balances. The COPS Office Staff Accountants also use the Federal Financial Report (SF-425) to compare the reported final expenditures with the actual final drawdowns to identify discrepancies that need attention. OJP currently uses its Grants Management System (financial reports), FMIS2 and GPRS to track undisbursed balances. OVW utilizes both FMIS2 data as well as data from OJP's GPRS to track undisbursed balances.

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

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

Department may utilize recoveries from the ARRA grants to cover any potential future reconciliation of debt. Unobligated balances were rescinded and transferred using the year-end closing module in Treasury by the end of October 2015.

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

OJP:

FY 2012: 5 accounts; \$485.6 in undisbursed and unobligated balances

FY 2013: 4 accounts; \$274.5 in undisbursed and unobligated balances

FY 2014: 4 accounts; \$94.1 in undisbursed and unobligated balances

FY 2015: 4 accounts; \$40.7 in undisbursed and unobligated balances

COPS:

FY 2012: 1 account; \$580.3 in undisbursed and unobligated balances

FY 2013: 1 account; \$277.5 in undisbursed and unobligated balances

FY 2014: 1 account; \$115.1 in undisbursed and unobligated balances

FY 2015: 1 account; \$84.4 in undisbursed and unobligated balances

OVW:

FY 2012: 1 account; \$63.2 in undisbursed and unobligated balances

FY 2013: 1 account; \$23.5 in undisbursed and unobligated balances

FY 2014: 1 account; \$11.1 in undisbursed and unobligated balances

FY 2015: 1 account; \$10.5 in undisbursed and unobligated balances