OIG Top Management and Performance Challenges Facing the Department of Justice – 2016

November 10, 2016

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 2016 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 nine challenges that we believe represent the most pressing concerns for the Department:

- Safeguarding National Security and Ensuring Privacy and Civil Liberties Protections
- Enhancing Cybersecurity in an Era of Increasing Threats
- Managing an Overcrowded Federal Prison System in an Era of Limited Budgets and Continuing Security Concerns
- Strengthening the Relationships Between Law Enforcement and Local Communities Through Partnership and Oversight
- Helping to Address Violent Crime Through Effective Management of Department Anti-Violence Programs
- Ensuring Effective Management and Oversight of Law Enforcement Programs and Promoting Public Trust
- Monitoring Department Contracts and Grants
- Managing Human Capital and Promoting Diversity With a Workforce Increasingly Eligible to Retire
- Using Performance-Based Management To Improve DOJ Programs

We believe safeguarding national security and enhancing cybersecurity in the wake of recent threats are particular challenges that will be at the forefront of the Department's attention and require vigilance in the foreseeable future. In addition, we have identified two of the challenges, helping to address violent crime and managing human capital while promoting diversity, as emerging issues that merit the Department's continued attention. Meeting all of these challenges will require the Department to develop innovative solutions and conduct careful monitoring of its efforts to achieve success.

We hope this document will assist the Department in its efforts to improve program performance and enhance its operations. We look forward to continuing to work with the Department to analyze and 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

Safeguarding National Security and Ensuring Privacy and Civil Liberties Protections

Countering the Terrorist Threat

As reflected in the recent attacks in New York and New Jersey, San Bernardino, and Orlando, terrorism remains a serious threat to the national security of the United States. The Federal Bureau of Investigation (FBI) has described this threat as "persistent and acute," and it continues to be listed by the Department of Justice (Department) as its top priority. The challenge for the Department is to protect the homeland from this threat, while also safeguarding privacy and civil liberties. In its proposed Fiscal Year (FY) 2017 budget, the Department allocates $6.5 billion to prevent terrorism and promote national security, including counterterrorism and counterintelligence efforts.

According to the Department, the Islamic State of Iraq and the Levant (ISIL) is creating "an unprecedented threat environment." ISIL uses Internet and social media campaigns to promote its ideology and recruit like-minded extremists to become foreign fighters in Iraq and Syria or to attack the West from within. Attacks in the United States by so-called homegrown violent extremists (HVE) on civilian targets increased in 2016, many of them reportedly motivated by ISIL propaganda. According to a Joint Intelligence Bulletin issued by the FBI, the Department of Homeland Security (DHS), and the National Counterterrorism Center, 10 of the 13 attacks and disruptions by HVEs between August 2015 and August 2016 were focused on civilian targets, as compared to 2 of the 18 attacks and disruptions that took place in the first 7 months of 2015.

Source: FBI website

Countering terrorist radicalization and recruitment and identifying HVEs before they engage in terrorist acts remains an exceptional challenge. FBI Director Comey recently acknowledged the magnitude of the task when he observed, "We are looking for needles in a nationwide haystack, but we are also called upon to figure out which pieces of hay might someday become needles." He also noted that "untangling the motivation" of the assailants is a very real challenge. Indeed, the tragic incidents highlighted above illustrate that the FBI continues to face the same challenges in locating and stopping attacks by HVEs that it did prior to the Boston Marathon Bombings in April 2013. One of the Boston attackers, Tamerlan Tsarnaev, was the subject of an earlier FBI assessment that was closed with no nexus to terrorism and was not reopened following his travel to Dagestan in 2012. A coordinated review in 2014 by four OIGs of information sharing prior to the Boston Marathon Bombings concluded that the U.S. government had information regarding Tsarnaev's travel, and that the travel was significant and warranted further investigation. As with the Boston attacks, the more recent attacks by HVEs highlight the difficulty the FBI faces as it receives information

about people who may pose a threat and then must determine which information is credible and worthy of additional investigation, an inquiry FBI agents must perform in each of the thousands of assessments conducted each year.

The Department has noted that social media is a critical tool that terror groups can exploit in recruitment efforts for both homegrown and internationally directed terrorism. Engagement with the private sector is crucial to ensuring that the Department understands the latest social media and online communication tools and maintains the ability to lawfully access information transmitted through them. In January 2016, President Obama announced the creation of a counterterrorism task force to thwart terrorists' use of social media. As part of this effort, Attorney General Lynch, Director Comey, and senior intelligence officials met with representatives of various U.S. technology companies to discuss ways to identify and remove extremist online content. According to news reports, Twitter, Microsoft, and Google have since implemented or are experimenting with ways to prevent terrorists from using their systems to communicate with others. In August 2016, Twitter reported that since the middle of 2015, it had suspended 360,000 accounts for violating the prohibition on making violent threats and promoting terrorism.

Balancing Security and Transparency Amid Global Threats

The Department faces a growing challenge as it seeks to engage and share information with private sector technology companies because of concerns raised by these companies about the privacy implications of the Department's requests for assistance. In some instances, these concerns have led to legal challenges. For example, as described in additional detail in the section on Cybersecurity, the recent dispute between the Department and Apple over obtaining access to information from the iPhone used by one of the San Bernardino attackers, highlights the challenge of obtaining investigative information from terrorists who communicate using encryption while protecting the privacy interests of law-abiding individuals. In another instance, Twitter recently sought to publish the number of secret orders it received from the government that required the company to turn over its customers' information, claiming that government-imposed restrictions on disclosing this information violated the company's First Amendment rights.

The disputes with Apple and Twitter, as well as the public debate about the appropriate scope of government surveillance, have highlighted the tension between security and transparency. The former Director of the National Security Agency, General Michael Hayden, explained the need to balance these considerations in this way: the federal government must provide the American people enough transparency to ensure that they understand what the government does to keep them safe without divulging so much information that it would hinder the government's ability to keep them safe.

The Office of the Inspector General's (OIG) oversight of the Department's counterterrorism efforts is intended to provide both transparency and accountability so that the public and policymakers can assess whether the Department is appropriately balancing privacy and security interests, and whether it is collecting and handling information in a manner that complies with federal law. For example, on June 2, 2016, the OIG submitted to Congress a classified version of a report on the FBI's use of Section 215 orders under the *Foreign Intelligence Surveillance Act* between 2012 and 2014, and its handling of non-publicly available information concerning U.S. persons received in response to these orders. An unclassified version of the report was released in September 2016. The report concluded that the process used by the FBI to obtain business records orders contained safeguards that protected U.S. persons from unauthorized collection, retention, and dissemination of information about them.

The Department's sharing of terrorist threat information and coordination of its operations with other entities involved in counterterrorism activities across the federal government also continue to be a focus of the OIG's oversight work. For example, as noted above, our office participated in a joint review with three other OIGs

of information sharing prior to the Boston Marathon Bombings. We currently are conducting a joint review with the Inspectors General of the Intelligence Community (IC) and DHS that focuses on the domestic sharing of counterterrorism information. This review will identify and examine the federally supported field-based intelligence entities engaged in counterterrorism information sharing to determine their overall missions, specific functions, capabilities, funding, and personnel and facility costs. The review also will determine whether counterterrorism information is being adequately and appropriately shared with all participating agencies and will identify any gaps and/or duplication of effort among the entities.


Source: OIG

Additionally, the OIG is conducting a review of the handling of known or suspected terrorists (KST) admitted into the federal Witness Security (WITSEC) Program. The review will examine practices for watchlisting and processing encounters with KSTs participating in the WITSEC program, and procedures for mitigating risks to the public through restrictions placed on this high-risk group of program participants. This is a follow-up review to our 2013 report, which found that the Department did not authorize the disclosure to the Terrorist Screening Center of new identities provided to KSTs and their dependents who were admitted into the WITSEC Program. This potentially allowed KSTs to use their new government-issued identities to fly on commercial airplanes and evade one of the government's primary means of identifying and tracking terrorists' movements and actions. Separately, the OIG has initiated a review of the FBI's efforts to protect seaports and maritime activity. That review is examining the FBI's roles and responsibilities for assessing maritime terrorism threats, preventing and responding to maritime terrorist incidents, and coordinating with DHS components to ensure seaport security.

The Department also faces a continuing challenge in countering the threat to the United States from foreign governments. For example, in August 2016, an FBI employee pled guilty to acting as an agent of China for providing restricted and sensitive FBI information to the Chinese government. Moreover, as we note in the Cybersecurity section of this report, recently DHS and the Office of the Director of National Intelligence identified Russia as directing a campaign of attacks intended to interfere with the U.S. election process. These examples highlight the importance of the Department remaining vigilant in its counterintelligence efforts against foreign adversaries to protect the nation's security.

Leveraging Emerging Technologies While Safeguarding Privacy

Concerns about the appropriate balance between security and privacy also will arise as the Department determines how to leverage emerging technologies that provide law enforcement with valuable information, such as geolocation or facial recognition technologies, while ensuring that the technology is used responsibly and lawfully. In 2013, the OIG released an interim report on the Department's use of Unmanned Aircraft Systems (UAS), or drones, in law enforcement operations and issued a final report in March 2015. The interim report found that in light of the technological capabilities of UAS, especially those raising unique privacy and evidentiary concerns, the Department should develop UAS-specific policies to guide the law enforcement components' use of this technology. In May 2015, the Department established policy guidance on the use of UAS, including privacy and civil liberties protections. Separately, in September 2015, the Department issued a new policy for the use of cell-site simulators that requires, among other things, that law enforcement agents obtain a search warrant before deploying the devices.

The effects of technology on Department operations were highlighted earlier this year when a senior Department official testified about the legal standards used by the Department to obtain various types of geolocation information. This official pledged that the Department is dedicated to ensuring that its policies and practices comply with applicable laws and uphold the Department's long-standing commitment to individuals' privacy and civil liberties. Continued oversight is required to ensure that the Department adheres to this commitment. For example, a report issued in May 2016 by the Government Accountability Office (GAO) found that although the Department has an oversight structure in place to help ensure the privacy of facial recognition data, the FBI did not update privacy guidelines for the system until 3 years after it began conducting facial recognition searches, and did not conduct sufficient testing to ensure the accuracy of search results. Given the sensitivity of biometric and geolocation data, and the proliferation of devices capable of capturing this type of information, the Department will need to ensure that its policies continue to evolve appropriately with technology.

Safeguarding national security must continue to be a top priority for the Department, and balancing this mandate with ensuring appropriate protection of privacy and civil liberties will continue to be a challenge. The Department has acknowledged that the challenges raised by modern technology are complex and that the agency will need to remain agile to address them. As both threats and technology evolve, the Department must continually reevaluate its national security efforts in order to appropriately safeguard the interests of the homeland and U.S. citizens.

Enhancing Cybersecurity in an Era of Increasing Threats

The cyber threat to the nation is growing and cyber intrusions are becoming increasingly commonplace, dangerous, and sophisticated. The FBI has stated that it continues to see an increase in the scale and scope of malicious cyber activity as measured by the amount of corporate data stolen or deleted, personally identifiable information compromised, and remediation costs incurred by victims. In order to protect the homeland in the digital age, the Department must continue to prioritize addressing these evolving cyber threats. Recent high profile cyber breaches, including those that reportedly may even have the potential to impact voting systems, demonstrate the importance of the Department remaining vigilant in combating cyber threats. Key to the Department's efforts will be its success in developing and maintaining a capability to identify the individuals or organizations responsible for intrusions. Challenges in this regard include the expanded use of encryption that can limit law enforcement from gaining access to critical investigative information and the recruitment and retention of technically-trained, highly-skilled cyber professionals to support the Department's cybersecurity mission. The Department must also take steps to guard against loss of data on its own computer systems. To this end, the Department's FY 2017 budget request provides $900 million to defend and protect Department networks, mitigate insider threats, investigate and prosecute criminal and terrorist cyber activity, and guard against identity and intellectual property theft and financial fraud, including a $175 million increase for FBI cyber investigation investments.

Strengthening the Nation Against Cyber Intrusions

Source: FBI website

Cyber intrusions that threaten the nation's security are among the highest priority matters investigated by the Department. One of the challenges for the Department in this area is detecting and deterring cyber intrusions before they occur rather than reacting to them after they have succeeded. Among the most dangerous cyberattacks are intrusions directed toward our national security, intellectual property, and democratic system by nation-states, nation-state sponsored hackers, global cyber syndicates, and so-called "botnets." According to FBI Director Comey, China, Russia, Iran, and North Korea present the most prominent nation-state cyber threats. As recently as October 2016, DHS and the Office of the Director of National Intelligence identified Russia as directing a campaign of attacks intended to interfere with the U.S. election process, with the goal of stealing and disclosing information intended to interfere with that process. This highlights the very serious potential consequences of a successful cyberattack. The stakes are high and, in an environment where actors are rapidly changing their tactics and techniques, the Department must ensure it remains agile in responding to cyber threats.

Given that the cyber threat is multi-faceted, the Department must continue to develop relationships with the private sector, state and local law enforcement, and global partners to effectively combat cyber threats. The frequency and impact of cyberattacks on the nation's private sector networks have increased dramatically in the past decade and are expected to continue to grow, making such partnerships between the public and

private sectors critically important. The *Cybersecurity Information Sharing Act of 2015* is intended to encourage companies to voluntarily share information about cyber threat indicators with federal, state, and local governments, as well as other private entities. However, as Director Comey observed in August 2016, it can be difficult to get the private sector to report system breaches to law enforcement. Sharing cyber incidents with the government (or other organizations) can expose a private company's network vulnerabilities and bring negative publicity, as well as create negative repercussions for multinational organizations that seek to do business in the very countries that may be sponsoring the cyberattacks.

Source: FBI website

The Department also faces challenges protecting its own systems. In response to the Office of Personnel Management (OPM) data breach in June 2015, the Department implemented various solutions to strengthen network security. This did not, however, prevent the February 2016 breach of Department data that exposed the contact information of 20,000 FBI employees. This "social engineering attack" was reportedly accomplished by a hacker posing as an employee to break into networks used by the Department's Civil Division by tricking staffers at an IT help desk into disclosing critical information. Department employees—the end users on the government's computer systems—are the first line of defense against cyberattacks of this type and the Department must continue to increase its security awareness in order to help thwart such threats.

Insider threats pose yet another cyber challenge to the Department. For example, as devices and technology become increasingly portable and outsourced, the Department's ability to detect and deter improper or unlawful activity by its employees will continue to be tested. President Obama signed an executive order in October 2011 requiring federal agencies to establish an insider threat detection and prevention program for their classified information. In accordance with this directive, the Department established such a program designed to detect patterns and indicators of insider threats. The OIG is currently examining the FBI's Insider Threat program to evaluate its ability to deter, detect, and mitigate insider threats. While the Department must be vigilant to detect insider threats, it must be careful not to allow such efforts to chill whistleblowers, who perform an important service to the Department and the public when they come forward with information regarding what they reasonably believe to be wrongdoing or mismanagement.

Unlocking Encrypted Messages to Fight Crime and Terrorism

Director Comey has stated that the growing use of encryption, which shields communications from all but those sending and receiving the messages, is one of the most pressing problems for law enforcement. As technology continues to evolve, the Department has sought to have the tools and methods it says it needs to gather evidence on terrorists and criminals who are increasingly using technology to hide their actions from law enforcement. For example, the FBI and others in law enforcement have said that investigations have stalled because of unlockable electronic devices. The FBI stated that in the first 10 months of FY 2016, it was unable to unlock 650 of 5,000 electronic devices investigators attempted to search. To address this challenge, the Department has requested $38 million for anti-encryption technology and research as part of its FY 2017 budget request. This issue recently attracted substantial public attention during the Department's legal battle to compel Apple to create special software to unlock the phone of one of the alleged terrorists

involved in the San Bernardino shooting. Department attorneys argued before a federal judge that law enforcement should be permitted to obtain an order requiring Apple to assist them with their investigation; attorneys for the company argued in response that, among other things, developing such a "back door" would have the effect of violating the privacy expectations of its customers and leave consumers vulnerable to hackers if the decryption tool fell into the wrong hands. The FBI successfully unlocked the San Bernardino phone with the assistance of a third party before the court rendered a decision in the dispute with Apple, but the broader issue and challenge remain.

The darknet presents another challenge for the Department in identifying criminals acting in an anonymous environment of increasing sophistication. The darknet is a part of the Internet that uses techniques, including special network configurations and encryption, allowing users to communicate anonymously. The darknet offers those attempting to evade law enforcement a means in which to commit a wide range of cybercrimes. These crimes can include hacking into non-authorized systems, disabling websites, or disseminating ransomware, which is malicious software used to lock the computer of an unsuspecting website visitor and require them to pay ransom to have their computer unlocked. The darknet can also shield individuals engaging in other criminal activities, such as child pornography and narcotics trafficking. It is difficult for law enforcement to identify individuals committing crimes using the darknet because they often use crypto-currencies such as Bitcoins, which allow users to remain anonymous. Although the FBI had success shutting down the Silk Road, a well-known darknet market for contraband, a successor darknet market reportedly soon replaced it, illustrating how important it will be for the Department to adjust to rapidly changing cyber environments.

Hiring Highly-Skilled Cyber Professionals

Attracting highly-skilled, technically-trained cyber professionals is a persistent challenge for the Department. Cyber professionals are in high demand in the private sector, potentially putting the government at a competitive disadvantage when it comes to recruiting these individuals. The FBI has noted that the significant salary gap between public and private sector positions can deter individuals from applying for jobs in the federal government and that many applicants are unable to pass the rigorous background investigation the FBI conducts on all potential employees. The pay gap and background screening issue have left the FBI often understaffed in this critical area. As we noted in a March 2016 report about an FBI computer forensic laboratory in New Jersey, the lack of qualified examiners with advanced training was a primary cause of the backlog of cases. It is imperative that the Department continue to develop new and creative hiring and retention strategies to attract highly skilled cyber professionals.

As the frequency and impact of cyber intrusions continue to increase and the nature of the attacks continues to change, the Department will be challenged to shift more of its efforts from reacting to attacks to preventing them. The Department must continue to prioritize resources to anticipate and prevent cyber intrusions, identify and investigate cyber actors before they strike, and engage with private sector partners and others in state and local law enforcement and abroad to accomplish this. And, while looking outward to protect from the cyber threat, the Department must also continue to focus on ensuring the security of its own computer systems and data. The Department must also marshal resources to address the impact of encryption, while at the same time recognizing and protecting civil rights and civil liberties. Finally, the Department faces the daunting challenge of creatively recruiting highly skilled cyber professionals to address these concerns.

Managing an Overcrowded Federal Prison System in an Era of Limited Budgets and Continuing Security Concerns

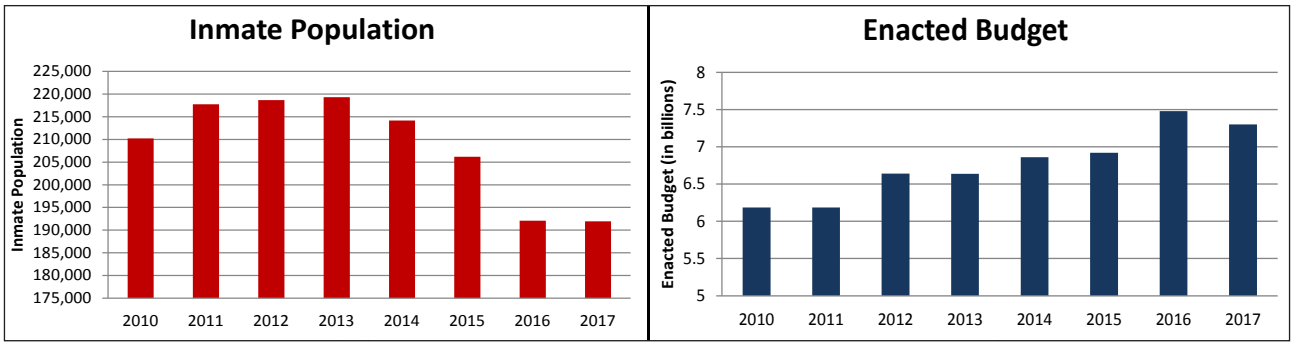
Confining offenders in prisons and community-based facilities that are safe and humane, while controlling costs and the size of the inmate population, is the constant challenge faced by the Federal Bureau of Prisons (BOP). While the inmate population has dropped 3 years in a row, falling to 192,170 at the end of FY 2016, overcrowding remains a challenge. As of September 30, 2016, BOP's institutions remained 16 percent over rated capacity, and high security institutions were 31 percent over rated capacity. This is a significant concern because more than 90 percent of high security inmates have a history of violence. The BOP's strategic plan says its goal is to achieve an overall overcrowding level "in the range of 15 percent." Thus, the Department continues to face a multi-faceted crisis in the federal prison system—addressing overcrowding while controlling spending and meeting the increasing resource needs of a changing inmate population.

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 continue to look for ways to contain costs. For the first time in recent years, the BOP has requested fewer funds for the FY 2017 budget—$7.3 billion—than the current funding level of $7.48 billion. Despite this, the BOP currently has the largest budget of any Department component other than the FBI, accounting for more than 25 percent of the Department's discretionary budget in FY 2016. Moreover, the cost of the prison system remains well above the $6.2 billion level of spending in FY 2010. Department spending on the federal prison system impacts its ability to fund other important Department operations, such as its critical law enforcement and national security missions. As such, it is imperative that the Department manage the prison system in the most cost-efficient manner possible.

Source: DOJ

To accomplish this, the Department must consider innovative solutions to contain costs. For example, inmate medical care continues to be a major part of BOP's overall spending, and is an area that needs to be monitored closely. From FY 2010 to FY 2014, BOP spending for outside medical services increased 24 percent, from $263 million to $327 million. A June 2016 OIG report found these rising costs were due, in part, to BOP being the only federal agency that pays for medical care without being able to rely on a federal statute or regulation that could limit BOP's reimbursement rates to those set by Medicare. In addition to rising medical costs, the BOP also is facing medical staffing shortages, as described in a March 2016 OIG report, which found that recruitment of medical professionals was one of the BOP's greatest challenges and that staffing shortages (a) limit inmate access to medical care, (b) result in an increased need to send inmates outside the institution for medical care, (c) contribute to increases in medical costs, and (d) can also impact prison safety and security.



Source: OIG

The Department must also take additional steps to ensure that it releases inmates when their sentences are complete. In a May 2016 OIG report, we found that of the 461,966 inmates released between 2009 and 2014, the BOP released 152 inmates from prison too late and 5 prisoners too early as a result to staff error. Being released late from prison is unjust and raises serious civil liberties concerns. Moreover, in addition to the enormous personal costs to inmates, these errors can result in additional litigation, settlement, and imprisonment costs, all borne by taxpayers.

Ensuring the Security of Inmates, Staff, and the General Public

The Department must continue its efforts to ensure the safety and security of staff, inmates, and the general public in federal prisons. In this regard, the smuggling of contraband into federal prisons remains a serious and significant problem, and addressing it must remain a high priority for the BOP. Preventing the physical and sexual abuse of inmates is also a critical safety responsibility for the Department, the role of which was expanded by the *Prison Rape Elimination Act of 2003*. Our Investigations Division continues to investigate allegations of contraband smuggling, bribery, and physical and sexual abuse of inmates by BOP employees. In FY 2016, these types of allegations resulted in 79 BOP employees receiving administrative sanctions or resigning while under investigation, and 50 BOP employees being convicted criminally.

In June 2016, the OIG evaluated BOP's contraband interdiction efforts and highlighted several areas the BOP must address in order to better tackle this problem. For example, our review found that the BOP's staff search policy lacks comprehensiveness to effectively deter staff from introducing contraband, which continues to pose a security concern to inmates, staff, and the public. From FYs 2012 to 2014, the BOP reported recovering over 21,000 contraband items in its institutions, including cell phones (the most common), narcotics, weapons, and tobacco. Another area of concern is BOP's operation of its armories, where prisons store emergency equipment such as firearms, ammunition, and other defensive gear. In a March 2016 report, we found weaknesses in BOP's armory controls that increased the risk that critical equipment could be lost, misplaced, or stolen. BOP needs to tighten these controls to reduce the risk of munitions and equipment falling into the wrong hands.

The Department faces similar challenges ensuring safety and security at its private or contract prisons. An August 2016 OIG report found that these prisons, which house mostly low security foreign national inmates, incurred more safety and security incidents per capita in a majority of the key categories we examined than comparable BOP institutions housing low security inmates. For example, in addition to a contraband seizure rate 8 times higher than that of BOP-run institutions, contract prisons also experienced higher rates of assaults both by inmates on staff and vice versa. The week after our report was issued, the Department announced it intends to phase out the use of contract prisons by either declining to renew current prison contracts or working to "substantially reduce" the scope of existing contracts. As efforts to phase out the use of contract prisons move forward, the Department will need to carefully manage the inmate population to ensure that it does not exacerbate overcrowding in BOP-run institutions.

Managing Department Programs That Also Can Impact Inmate Population Numbers

Further compounding BOP's challenge to ensuring inmate safety and security is the continued overcrowding of the federal prison system. This problem cannot be addressed by the BOP alone, given that it has little control over the number of inmates it is charged with safely housing. Rather, multiple Department-level efforts may impact the overcrowding and cost concerns facing the federal prison system. In August 2013, the Department launched its Smart on Crime initiative with the goal of reforming the federal criminal justice system by, among other things, curbing reliance on incarceration for less dangerous offenders. Proposed reforms include requiring U.S. Attorneys' Offices (USAO) to modify their guidelines for when federal prosecutions should be brought, limiting the use of mandatory minimums and enhancements for repeat low-level, non-violent drug defendants, and enhancing prevention and reentry efforts at each USAO. In December 2015, the OIG initiated a review of the Department's implementation of certain principles regarding prosecution and sentencing reform it announced in its Smart on Crime initiative.

Source: DOJ

As part of Smart on Crime, federal prosecutors are encouraged to consider alternatives to incarceration, such as pretrial diversion and diversion-based court programs, in appropriate cases involving non-violent offenders. In July 2016, the OIG released an audit that found the Department cannot fully measure the success of its diversion programs because neither the Executive Office for United States Attorneys (EOUSA) nor the USAOs are adequately tracking this information. Furthermore, we found a wide disparity between how often these programs are used by different USAOs. For example, while one district diverted as many as 326 defendants, other districts diverted none. In line with the OIG's findings, the GAO echoed the same concerns in its own June 2016 report on the Department's use of alternatives to incarceration. Mirroring our findings, the GAO report also suggested that the Department would benefit if it could better measure the success of its different pretrial diversion programs.

Another area where the Department can make strides is by improving how the BOP prepares inmates for release into the community. During the past 3 years, the BOP has released nearly 125,000 federal inmates into residential reentry centers, home confinement, or directly into communities. Although the BOP invests a considerable amount of money each year into its reentry programs and requires that most sentenced inmates participate in its Release Preparation Program (RPP), the OIG found in an August 2016 review that it has no performance metrics to determine whether its RPPs are successful. In fact, the last BOP study on the overall recidivism rate for federal inmates occurred more than 20 years ago. The BOP must begin measuring both the overall recidivism rate for federal inmates, as well as how successful each prison has been in preparing inmates for release, so the Department can better determine which facilities and programs deserve to be funded and expanded, and which programs should be ended. The good news is the BOP told us it is currently working on a study to fill this knowledge gap and that, for the first time since 1994, it aims to release recidivism rates in FY 2017.

Although the Department makes clear that its Clemency Initiative, announced in April 2014, is not intended as a means to reduce the number of inmates, grants of clemency have an effect on the inmate population. As conceived, the Department said it would prioritize clemency applications for non-violent, low-level offenders. In February 2016, the OIG initiated a review of the Department's handling of the executive clemency process, with an emphasis on assessing the procedures followed by the Department and the impact

of the Department's new criteria for prioritizing commutation petitions. While our review is ongoing, the number of inmates granted clemency by the President has increased significantly this past fiscal year, with 95 inmates granted clemency in March, 58 inmates in May, 42 inmates in June, and another 325 in August. As FY 2016 came to a close, the President had commuted 583 sentences, compared to 79 the year before.

Another program that has the potential to impact the prison population is the Department's Compassionate Release Program. In August 2013, the BOP announced, as part of the Smart on Crime initiative, that it was expanding its criteria for inmates seeking compassionate release to include elderly inmates. This change allowed inmates age 65 and older, of which there were 4,384 in BOP custody at the time, to request a reduction in sentence if they meet certain criteria. However, our subsequent report on the BOP's aging inmate population, released in May 2015, found that during the first year the new BOP policy was implemented only 2 of the 348 inmates who applied were released under the new provisions. While the number of inmates released under these provisions in FY 2015 increased, in FY 2016 the BOP released only 5 inmates, despite a 65-percent increase in applications. In February 2016, the Inspector General appeared before the U.S. Sentencing Commission and highlighted the concerns we expressed in our report about the age and time served requirements. The Commission adopted significant changes to the U.S. Sentencing Guidelines addressing these issues in April 2016. We will continue monitoring the program to determine whether these changes lead to more use of compassionate release for appropriate inmates.

Another Congressionally-authorized program that could impact the federal inmate population if managed successfully is the International Prisoner Transfer Program, which allows the Department to transfer foreign inmates to their host nations to serve their prison sentence. In an August 2015 status report, the OIG found that the number of inmates transferred under the program had actually decreased since our prior report in 2011, despite a substantial increase in the number of inmates applying for such transfers. Using FY 2013 BOP annual cost data, we found that BOP could potentially save $4.5 million by transferring just 1 percent of inmates who applied and were ultimately transferred. The OIG's status report recommended that Department leadership boost the effectiveness of this program by actively engaging with treaty transfer partners, and the Department has since taken some steps to encourage treaty nations to accept more inmates. Yet, despite its efforts, over the past 3 years the number of foreign nationals transferred to treaty nations has sharply declined. In fact, since FY 2014, the Department has transferred just 436 inmates (averaging 145 inmates per year), its lowest total in more than a decade, down from the 227 per year average between FY 2011 and FY 2013.

The operation of the federal prison system presents a host of continuing challenges for the Department. While it has taken positive steps in some areas, such as its plan to determine and release recidivism rates that will help it evaluate the efficacy of its programs, there is still substantial progress to be made. Indeed, BOP will need to make progress on a number of fronts if it is to achieve its mission of confining offenders in "prisons and community-based facilities that are safe, humane, cost-efficient, and appropriately secure, and that provide work and other self-improvement opportunities to assist offenders in becoming law-abiding citizens."

Strengthening the Relationships Between Law Enforcement and Local Communities Through Partnership and Oversight

Recent shootings by, and of, local law enforcement officers have raised serious questions about the relationship between law enforcement and the communities they serve. As Attorney General Lynch recently observed, the loss of life among civilians and law enforcement, "brings pain not just to individual communities, but to our entire nation." The Department's burden continues to be to determine how best to assist in solving a problem that manifests itself locally, yet has an indisputable effect on the Department, federal law enforcement, and the country as a whole. There are at least five ways where the Department plays a critical role in this area: (a) creating an effective data collection system to accurately understand police use of deadly force; (b) partnering with state and local governments, and local law enforcement agencies, through grants programs; (c) monitoring and assisting with the reform of police departments that are found to have engaged in a pattern or practice of unlawful or unconstitutional misconduct; (d) investigating and prosecuting law enforcement officers, whether local, state, or federal, who violate federal civil rights laws; and (e) assisting in the response to civic unrest as needed when an incident of police-community violence does occur. The challenge for the Department is how to address these areas when it has limited resources to use, limited jurisdiction upon which to act, and limited impact over local crime fighting.

Compiling Accurate and Complete Data on Law Enforcement Shootings

Source: OJP website

For government decision-makers and the public to better understand the issues raised by law enforcement shootings, there needs to be data that adequately measures the nature and scope of the issue. The *Violent Crime Control and Law Enforcement Act of 1994* requires the Department to collect "data about the use of excessive force by law enforcement officers" and issue an annual report regarding such data. In addition, pursuant to the Death in Custody Reporting Act, state and local law enforcement agencies face grant funding reductions if they do not report to the Department information regarding the death of any person while in law enforcement custody, including while under arrest. Nonetheless, the Department has historically struggled to collect adequate data regarding officer-involved shootings and excessive use of force by law enforcement officers, because state and local law enforcement agencies are not legally required to provide such data to the federal government. Thus, FBI Director Comey has emphasized that the Department needs "more and better information," including better data "related to officer-involved shootings...and attacks against law enforcement officers," which he said would help inform the "passionate, important conversations" we are having "in this country about police use of force."

In October 2016 Attorney General Lynch announced that the Department has taken several steps toward improving its collection of this critical data. These include: (a) the FBI's partnership with local, state, tribal, and federal law enforcement to create a National Use-of-Force Data Collection Program, which is expected to be piloted in early 2017 and include data regarding instances where a law enforcement officer discharges a firearm at a person as well as instances where the use of force results in death or serious bodily

injury; (b) the Bureau of Justice Statistics issuance of a draft proposal outlining its plan for collecting death-in-custody data from state and local law enforcement agencies; (c) the Attorney General's issuance of a memorandum to federal law enforcement agencies notifying them of their obligation to comply with the *Death in Custody Reporting Act*, beginning with FY 2016 data; and (4) the creation of a new Office of Community Oriented Policing Services (COPS)-administered Police Data Initiative that will collect and publicly release data from law enforcement agencies regarding stops and searches, uses of force, and officer-involved shootings.

The Department's challenge will be to collect and organize the data collected through each of these efforts to improve the nation's understanding of this problem, and to help local, state and federal law enforcement search for creative solutions based on this information. In that regard, complete, timely, and reliable data is essential so that the nation may have informed policy discussions about this subject.

Using Grants To Assist Local Law Enforcement With Hiring, Equipment and Training

One of the Department's greatest challenges is to figure out what state and local efforts to support and how to best do so with its limited resources. The primary method it has relied on to date is to partner with state and local law enforcement by offering grants for hiring, equipment, training, research, and other efforts to assist them and improve police-community relations. By offering grants to local communities from COPS, Office of Justice Programs (OJP), and Office on Violence Against Women (OVW), the Department has the potential to provide important assistance to local law enforcement. For example, the COPS Hiring Program recently announced $119 million for hiring community policing officers. This year's grants mark over $14 billion to advance community policing since 1995, with approximately 129,000 police positions funded. The challenge for the Department is to ensure that its grant funds are wisely spent and promote sustainable and effective initiatives so as to maximize the impact in assisting communities in preventing violence between police and communities.

Source: COPS website

Body cameras used by state and local law enforcement have the potential to assist in furthering transparency and accountability in encounters between citizens and the police. Last year OJP awarded nearly $20 million to law enforcement agencies in 32 states through the *2016 Body-Worn Camera Policy and Implementation Program*. Through such programs, we believe the Department should continue working to ensure that its limited grant funding is being used to support positive reforms in local policing.

Another challenge for the Department is to look for ways to help local law enforcement standardize its training and practices to aid with the safe and effective fulfillment of their responsibilities, strengthen professionalism, and thereby enhance the ability to reduce community tensions. Both OJP and COPS have developed technical assistance programs that target improving police department practices and community relations. Specifically, OJP's Diagnostic Center provides systems analysis and recommendations related to improving or deploying data to drive justice reform, such as assessing early intervention systems to improve officer accountability. Under the Collaborative Reform Initiative, COPS provides a more comprehensive assessment of requesting police departments' operations to identify issues that may affect public trust, including use of force practices, and issues public recommendations consistent with best practices in policing. A similar but separate COPS effort, the Critical Response Technical Assistance program, offers

a more focused assessment of how police departments handle procedures related to particular high-profile events and incidents or sensitive issues. And lastly, the Department has announced its intention, as part of some training grants, as well as through internal training for the four federal law enforcement components and Department attorneys, to address the issue of implicit bias at all levels in the justice system. To multiply the effect of its prevention dollars, the Department might consider providing grants for law enforcement agencies to obtain accreditation through recognized providers to supplement efforts to increase professionalism and improve community relations. Such an initiative may fit with the recent efforts at direct outreach by Attorney General Lynch during her nationwide community policing tour.

Providing Oversight through Pattern or Practice Investigations

While it seeks ways to assist local police departments through its grants, the Department also plays a critical oversight role through its Civil Rights Division (CRT) in ensuring that police departments act in accordance with the Constitution and federal statutes. CRT investigates law enforcement agencies across the nation to address allegations of excessive force; unlawful stops, searches, or arrests; and discriminatory policing. Under the *Violent Crime Control and Law Enforcement Act of 1994*, it is unlawful for law enforcement officers to engage in a pattern or practice of conduct that deprives individuals of rights protected by the Constitution or federal statutes, and the Department may initiate a civil action when it has reasonable cause to believe that such conduct has taken place. Thus, under 42 U.S.C. § 14141, CRT conducts "pattern or practice" investigations through which it endeavors to address local issues and create models for effective and constitutional policing nationwide. With approximately 18,000 state and local law enforcement agencies throughout the country, however, the challenge for CRT is to identify where and how it can best target Departmental attention and resources to maximize its impact. In the past 7 years CRT has opened "pattern or practice" investigations on 23 police departments across the country, and is currently enforcing 17 agreements with law enforcement agencies, including 14 consent decrees and one post-judgment order. The OIG is currently conducting an audit of CRT's efforts to address patterns or practices of police misconduct, including how CRT identifies and selects matters for investigation, the role of the Department's grant programs in addressing or preventing such conduct, and how these efforts are coordinated.

The challenge for CRT is to be able to select and conduct investigations and enforce resulting consent decrees in ways that effectively address unconstitutional practices, ensure accountability, and increase community confidence in both local law enforcement departments with high-profile problems and those with less well known issues. Further, transparency in the CRT process can assist other local law enforcement entities in assessing and improving their own operations.

Investigating and Prosecuting Violations of Federal Civil Rights Laws

In addition to helping reform troubled police agencies through grants and oversight, the Department, through CRT's Criminal Section and USAOs around the country, also prosecutes law enforcement officers for violating individuals' civil rights. During the last 8 years, the Department has charged more than 480 defendants, most of whom were local, state, and federal law enforcement officers, with committing willful violations of constitutional rights under color of law and related offenses. Here, too, the Department must determine how to best use its limited resources in what are resource-intensive cases. In doing so, the Department must carefully consider where federal investigation and prosecution is appropriate, taking into account local conditions and interests and the state or local jurisdiction's ability and willingness to prosecute effectively, as laid out in United States Attorneys' Manual Title 9-27.240. The challenge for the Department then is to determine when federal intervention is warranted in these difficult and often high-profile cases.

Providing Support To Communities in Emergency Situations

Source: CRS website

Finally, if prevention fails and civic unrest directed at local law enforcement threatens or begins to unfold, the Department faces the challenge of effectively using its limited resources to provide conciliation services and to ensure they are effective in addressing difficult local situations. The Department's Community Relations Service (CRS), created by the *Civil Rights Act of 1964*, is authorized to provide emergency response support through the deployment of conciliators to affected communities. As CRS's Strategic Plan notes, "timing is essential in preventing community tensions from erupting into violence." However, CRS is a relatively small Department component, with a staff allocation of 74 employees, 28 positions currently unfilled, and a budget of $14.5 million in FY 16. Ensuring appropriate and effective deployment of these limited resources, at a time when numerous communities are facing these issues, is an important challenge for the Department.

Ultimately, the Department must work through all these critical issues to determine how to optimally use its limited but substantial resources and personnel to help improve the relationship between law enforcement and the public they serve. Through effective data collection tools, efficient and effective use of grant programs, oversight through pattern or practice investigations and criminal prosecutions where warranted, and response support when needed, the Department can act in multiple ways to strengthen relationships among law enforcement and the communities they serve. These efforts, if successful, can maximize the safety of citizens while protecting the Constitutional rights guaranteed to all Americans.

Helping to Address Violent Crime Through Effective Management of Department Anti-Violence Programs

While state and local law enforcement has primary responsibility for addressing street crime, including in responding to the increases in violent crime that certain communities in our nation are facing, the Department plays an important role in those efforts. Indeed, the Department's strategic plan identifies combating violent crime as one of four "priority goals" and the Department has a number of initiatives underway to accomplish this. These include law enforcement efforts by the Department's law enforcement components and USAOs; technical assistance to state, local, and tribal governments by law enforcement and grant-making components; and grant funding for a wide array of violence-related issues and programs through OJP, OVW, and COPS. For example, the FBI operates more than 160 Safe Streets Task Forces that partner with state and local law enforcement to investigate gang and drug-related violent crime, and the Bureau of Justice Assistance has created the Violence Reduction Network, which is designed to provide enhanced technical assistance and other services to select cities that are addressing serious problems with violent crime. In addition, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) has made addressing violent crime a leading priority and has established task forces focused on gang and firearms-related violence. The Department also has placed increased emphasis on violence prevention and reentry programs through its "Smart on Crime" initiative.

Source: OJP website

The United States as a whole currently is enjoying some of the lowest reported rates of crime and violent crime in decades, with the overall crime rate reported by the FBI for 2015 roughly half of what it was in 1990. Unfortunately, despite such reductions in nationwide reported crime rates, many neighborhoods remain plagued by violence. Areas within localities such as Baltimore, Chicago, Detroit, East St. Louis, and Flint continue to face the problem of entrenched violence, each with reported rates of crime that are many multiples of the national average. Overall, the reported murder rate rose nearly 11 percent nationally in 2015. But in some cities the increases were far more dramatic, such as Baltimore which experienced nearly a 63 percent increase to approximately 55 murders per 100,000 inhabitants. Gangs—national and neighborhood-based—contribute significantly to the violence problem. According to the 2015 National Gang Report from the FBI-sponsored National Gang Intelligence Center, gangs continue to grow, and they are expanding their criminal activities, thus posing "a significant threat to law enforcement and to the communities in which they operate."

In addition to the incalculable loss of human life, in some neighborhoods residents live in fear of being caught in the crossfire of gang fighting, exacting a significant social and economic cost. According to researchers at the University of Chicago, the total annual social and economic cost to the City of Chicago and its residents related to violence of this sort totals in the billions of dollars. Similarly, researchers at Temple University have evaluated the harms that gangs inflict on communities and identified 16 characteristics other than violence; these include economic factors, fear from intimidation, and interference with schooling.[1]

[1] Ratcliffe, Jerry H., Harms of Violent Street Gangs - How Do Gangs Harm Their Communities (October 10, 2015) at 1.

Americans are highly cognizant of the harm caused by violent criminals. A Gallop poll taken in April 2016 showed that concern over crime had reached a 15-year high, with 53 percent of poll respondents stating that they worried "a great deal" about crime and violence. As Attorney General Lynch noted in September 2016, "nothing threatens the vibrancy of our communities and the well-being of our people as severely as violence. Violent crime endangers lives, destroys families and paralyzes neighborhoods. It stifles opportunity and spreads fear. It deters investment and discourages education."

The OIG in the past has evaluated aspects of the Department's management of its anti-violence programs. For example, we have evaluated the level of coordination between the Department's violent crime task forces; ATF's implementation of its Violent Crime Impact Team initiative, which was designed to reduce homicides and other firearms-related violent crimes; and the intelligence and coordination activities of the National Gang Intelligence Center and the National Gang Targeting, Enforcement, and Coordination Center. In each of these reviews we identified important areas for improvement.

In an environment of limited government resources, we believe that it is essential for the Department to pay especially close attention to its stewardship of its anti-violence resources in light of the stakes involved. In order to better understand the Department's approach to management of its current violent crime initiatives, the OIG has initiated a review that is examining the Department's strategic planning and accountability measures for combating violent crime. Strategic planning is a basic management discipline used by businesses and the military, as well as law enforcement agencies, to help ensure that limited resources are directed to the most pressing problems and effectively disbursed. There are numerous examples of these efforts in the violent crime area, such as the strategic plan and implementation measures developed by the Memphis Shelby Crime Commission in Memphis, Tennessee, and the planning process employed by UnifiedErie, a community effort to reduce crime and violence in Erie, Pennsylvania. These and other examples show the many benefits of planning, including improved decision making and performance and, as a leading academic in the field of strategic planning has described, the creation of "significant and enduring public value."[2]

Source: UnifiedErie website

Our pending violent crime review is examining planning activities throughout the Department, to include the law enforcement and grant-making components, Main Justice, and USAOs, and attempting to better understand how the Department is evaluating risk and allocating its violent crime resources. Among the issues we are examining more closely are whether the FBI's own advances in planning techniques might offer some important lessons for the Department as a whole, how the Department has conceived the role of U.S. Attorneys in the fight against violent crime, and whether the tens of millions of dollars that the Department distributes in grants each year are being effectively coordinated within the Department. While local law enforcement clearly has the lead role in efforts to address violent crimes on the streets of our communities, the unique role the Department plays in assisting those efforts through its law enforcement and grant-making components makes it essential that the Department's programs be carried out effectively and efficiently. We expect our review to assist the Department in those efforts.

[2] See John M. Bryson, Strategic Planning for Public and Nonprofit Organizations 4th Ed. (San Francisco, CA: Jossey-Bass), 8.

Ensuring Effective Management and Oversight of Law Enforcement Programs and Promoting Public Trust

The Department is tasked with the Attorney General's highest priorities; among these are enforcing the law, defending the interests of the Unites States, and seeking just punishment for those guilty of unlawful behavior. It relies on the services of over 110,000 employees to manage federal law enforcement programs and meet its mission of ensuring public safety. The same leaders and supervisors responsible for carrying out the crucial mission of the Department are also tasked with responsibility for effective management and oversight of these law enforcement programs and ensuring ethical conduct. The issue of oversight continues to challenge Department supervisors, and how they undertake this responsibility affects whether the Department will be seen by the public as one abiding by high ethical standards; run effectively and within the rules.

Ensuring Effective Management and Oversight of Law Enforcement Programs

Federal law enforcement programs require effective planning, management, and oversight. The inherent risks associated with many of these programs must be balanced with the public's safety, as well the privacy and civil rights of individual citizens. Strong leadership, adept supervision, and effective management are essential elements of this balance. The examples described below illustrate the importance of these efforts.

Source: DOJ

Confidential Source (CS) and Confidential Informant programs are the backbone of federal law enforcement agencies, yet managing these programs has been and continues to be a significant challenge facing the Department. The Attorney General's Guidelines Regarding the Use of Confidential Informants (AG Guidelines) provide guidance to all Department law enforcement components on establishing, approving, utilizing, and evaluating sources. Yet, in the past 4 years, our reviews have found that two of the Department's law enforcement components, the Drug Enforcement Administration (DEA) and ATF, were not in full compliance with the AG Guidelines.

For example, the OIG's July 2015 audit of the DEA's CS Policies and Oversight of Higher-Risk CSs found that the Criminal Division's 2004 approval of the DEA's confidential source policies allowed the DEA to differ in several significant respects from the AG Guidelines' requirements. The DEA's differing policies for reviewing, approving, and revoking CSs' authorization to conduct "otherwise illegal activity" have resulted in DEA personnel being able to use CSs to conduct high-risk activities without the level of review that the AG Guidelines would otherwise require. More recently, our September 2016 audit of the DEA's oversight and management of its confidential source program found that between FYs 2011 and 2015 the DEA did not adequately oversee payments to its sources, which exposed the DEA to an unacceptably increased risk for fraud, waste, and abuse. This is particularly true given the frequency with which DEA offices utilize and pay confidential sources. We found that the DEA had over 18,000 active confidential sources assigned to its domestic offices, with over 9,000 of those sources receiving approximately $237 million in payments for information or services they provided to the DEA. We also estimated the DEA may have paid about $9.4 million to more than 800 previously deactivated sources during that same 5-year period. In addition, we found problems related to the DEA's use of "Limited Use" sources, who are deemed by the DEA to be low-

risk and thereby needing less supervision than other sources. Our review showed that the DEA signed up employees of Amtrak and the Transportation Security Administration (TSA) as Limited Use sources, despite the fact that the DEA could have obtained the information provided by these sources at no cost to the DEA. In January 2016, our Investigations Division reported that a single Amtrak employee was paid $854,460 over a 20-year period ending in January 2014 thereby wasting substantial government funds. Our audit, meanwhile, found that between FYs 2011 and 2015, the DEA paid at least 33 Amtrak employees a total of $1.5 million and 8 TSA employees a total of more than $94,000.

The DEA is not alone in struggling in this critical area. In our 2012 review of ATF's Operation Fast and Furious, we determined that the Department had never amended the AG Guidelines to include ATF in its coverage, even though ATF became a part of the Department in 2003. Our report recommended that the Department examine ATF's policies to ensure that they were in compliance with the AG Guidelines and other Department policies. In a follow-up review that the OIG released in February 2016, we noted that the Department believed that ATF's law enforcement policies complied with DOJ policies with three exceptions, each of which were addressed with revisions to ATF policy. The OIG is currently performing an audit of the ATF's management and oversight of its confidential informants.

To effectively protect Americans at home, the Department's law enforcement components often must partner with foreign nations and conduct operations overseas. The relationships that these agencies forge with international law enforcement are essential to the Department's mission but provide unique challenges for the components. In order to conduct successful and often complex investigations of sophisticated criminal targets, agencies within the Department often use extensive undercover or other long-term investigative operations or the expenditure of substantial funds in operation specific areas. However, in recent years, questions have been raised regarding some of these operations. The OIG, in collaboration with the Department of State (State) OIG, is conducting a review of the post incident responses by State and the DEA to three drug interdiction missions in Honduras in 2012, all involving the use of deadly force. The review, among other things, addresses pertinent pre-incident planning, the rules governing the use of deadly force, the cooperation by State and DEA personnel with post shooting reviews, and the information provided to Department leadership, Congress, and the public regarding the incidents.

The Department's law enforcement components also must be reasonable stewards of Department resources with regard to overseas operations. As discussed in more detail in the section on Contracts and Grants Oversight, in March 2016 the OIG found that the DEA expended nearly $8.6 million to purchase a large aircraft to support its counternarcotics efforts in Afghanistan, and that 7 years after purchase, it was inoperable and had never flown to Afghanistan. The DEA's inefficient use of its aviation assets coupled with the number of mission requests declined by the DEA raised serious questions as to whether the DEA was able to meet the operational needs for which its presence was requested in Afghanistan.


Source: DOJ

The Department has a zero tolerance policy for sexual harassment, and it is imperative that the Department's law enforcement components, in rule and practice, comply with this policy. Essential to ensuring that this policy is made a reality is the handling of sexual harassment complaints. In March 2015, the OIG issued a report on the handling of sexual harassment and misconduct allegations by the Department's four law enforcement components. The OIG identified systemic issues in the processes for handling such allegations at the DEA, FBI, U.S. Marshals Service (USMS), and ATF. Specifically, the OIG found that although ATF and the USMS had clear policies requiring supervisors to report misconduct allegations, supervisors sometimes failed to report such allegations, even when the allegation was similar to past misconduct. Further, the DEA's reporting policies did not clearly delineate what should be reported to

headquarters officials. As a result, DEA supervisors exercised discretion in deciding what to report. Another ongoing OIG review of the handling of sexual harassment and misconduct allegations in the Department's Civil Division will assess how that division responds when allegations of this kind are made against its employees. Separately, the OIG has begun a review of the related issue of gender equity in the operations of the four law enforcement components. In this review, we intend to assess component demographics, gender discrimination complaints, and the complaint process, as well as staff perceptions related to gender equity and the reasons for those perceptions.

Promoting Public Trust by Ensuring Ethical Conduct

As the federal agency charged with protecting the safety, civil rights, and freedom of American citizens, the Department and its employees must uphold the highest ethical traditions. Over the past year, the OIG has investigated law enforcement agents and attorneys for a wide range of criminal and administrative misconduct, ranging from misuse of power, acceptance of bribes, improper gifts and favors, and harassment. As detailed below, such misconduct erodes public confidence in the integrity of law enforcement and may have a significant negative impact on the Department's prosecutions.

Source: DOJ

With their power to make arrests and carry firearms, law enforcement agents are expected to not only enforce the law, but also follow it themselves. When they fail to meet the high expectations of the citizenry, it not only harms the Department's reputation, but also can impede programs and result in greater distrust of all law enforcement. The challenge for the Department is to provide effective supervision to try to prevent these incidents from occurring and, when they do, to locate and stop the behavior as quickly as possible and minimize its impact on the Department's law enforcement efforts and the public at large.

As reflected in a number of recent OIG investigations, Department employees are engaging in increasingly complex types of wrongdoing, thereby increasing the Department's challenge in deterring such misconduct. Several OIG criminal investigations illustrate the point, including an embezzlement of Bitcoins by a DEA agent and U.S. Secret Service agent, the theft of heroin by an FBI agent, and a conflict of interest by a former senior FBI official.

When Department attorneys commit misconduct unrelated to their legal work, the OIG has jurisdiction; and, in the past year, we have investigated a wide range of allegations of such wrongdoing by the Department's attorneys. For example, OIG investigations found that a U.S. Attorney violated Department regulations on political activities and fundraising and lacked candor in interviews with the OIG about those activities; and that a U.S. Attorney violated Department rules on the use of government travel cards. In addition, the OIG found that a U.S. Attorney had an inappropriate relationship with a subordinate, including sending multiple harassing e-mails and communications to the employee and then encouraging the employee not to cooperate with the OIG investigation and lying to Department officials about the underlying conduct. In another OIG investigation, we determined that an Assistant U.S. Attorney made unwanted sexual advances towards three female USAO employees while attending training.

To ensure transparency regarding our investigations, the OIG regularly posts summaries of employee misconduct findings on its website, including those involving federal prosecutors and employees from throughout the Department, including all four law enforcement components, who are members of the Senior Executive Service or level GS-15 and above.

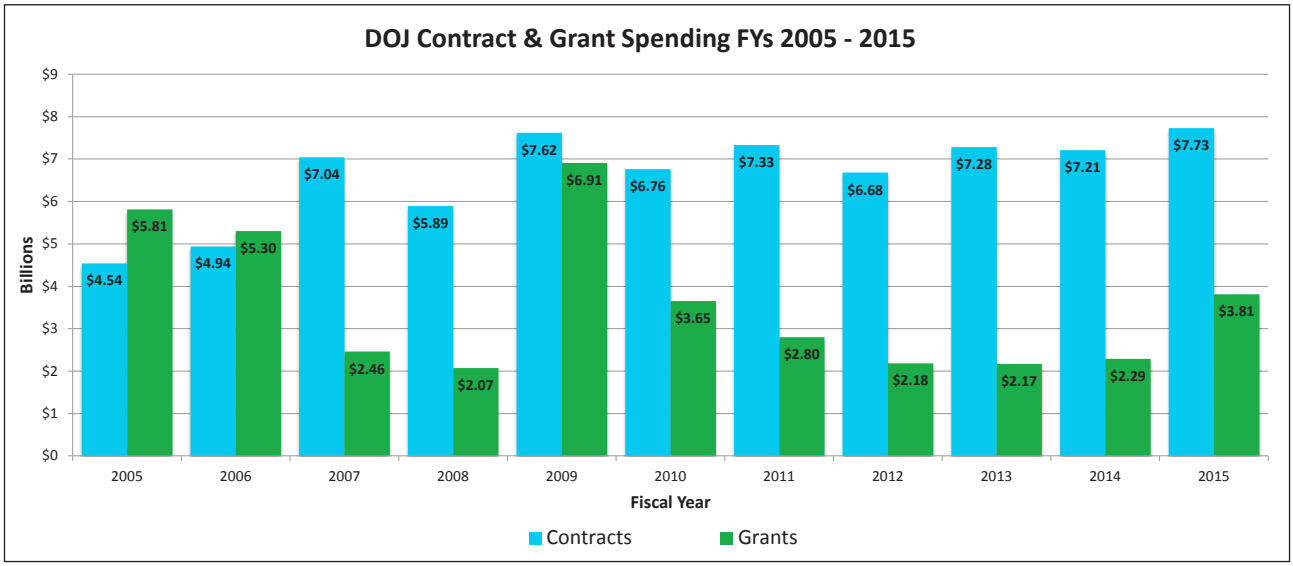
The OIG, however, does not have authority to investigate allegations of misconduct against Department attorneys when the allegations are related to their work as lawyers. Those allegations fall under the exclusive jurisdiction of the Department's Office of Professional Responsibility. The OIG has long believed that there is no principled basis for this continued limitation on our jurisdiction, and no reason to treat the investigation of misconduct by prosecutors differently than misconduct by agents. Under the current system, misconduct allegations against agents are handled by a statutorily independent OIG, while misconduct allegations against prosecutors are handled by a Department component that lacks statutory independence and whose leadership is both appointed by and removable by the Department's leadership. Bipartisan bills pending in both the U.S. House of Representatives and the U.S. Senate would remove this limitation on the OIG's jurisdiction. The legislation, as now proposed, would allow the OIG to investigate these important matters, where appropriate, with the independence and transparency that is the touchstone of all of the OIG's work, thereby providing the public with confidence regarding the handling of these matters. The Department's attorneys should be held to the same standards of oversight as other Department components, and the OIG should have oversight over all Department employees, just like every other OIG.

In response to a draft of this report, the Department questioned our position that the OIG should have the same authority as every other federal Inspector General to review allegations of misconduct by Department attorneys in connection with their work as lawyers. Among other things, the Department took issue with our description of OPR's relative lack of independence as compared to the OIG by asserting that (1) OPR's Counsel "remains unchanged with successive Attorneys General and presidential administrations," (2) the OIG has not "criticized OPR's work, the thoroughness of its investigations, or the soundness of its findings," and (3) the OIG has not "identified a single OPR investigation that failed to appropriately hold accountable . . . Department attorneys." On the first point, the same could be said of supervisory attorneys throughout the Department and, in fact, contrary to the Department's claim with regard to OPR, in April 2009, less than 4 months after the last change in presidential administrations, the new Attorney General replaced the OPR Counsel without any public explanation. On the second and third points, neither the OIG nor the public are in a position to fully assess the thoroughness and soundness of OPR's work precisely because OPR does not disclose sufficient information to allow for such an assessment. However, federal judges, the American Bar Association, and the Project on Government Oversight (POGO) have all questioned the level of independence, transparency, and accountability of OPR. *See, e.g.,* Order by Hon. Emmet G. Sullivan Appointing Henry F. Schuelke Special Counsel in United States v. Stevens, No. 08-cr-231 (Apr. 7, 2009), p. 46. ("*the events and allegations in this case are too serious and too numerous to be left to an internal investigation that has no outside accountability*") ; "Criminal Law 2.0," by Hon. Alex Kozinski, 44 Geo. L.J. Ann. Rev. Crim. Proc. iii (2015); ABA Recommendation urging the Department of Justice to release "as much information regarding individual investigations as possible," Aug. 9-10, 2010, available here; "Hundreds of Justice Department Attorneys Violated Professional Rules, Laws, or Ethical Standards: Administration Won't Name Offending Prosecutors," Report by POGO, March 13, 2014, available here.

Moreover, whatever the soundness of OPR's work, the Department's efforts to equate OPR's independence and transparency with that of the OIG flies directly in the face of the *Inspector General Act*, which fundamentally exists to create entities with an enhanced degree of independence and transparency so that they can credibly conduct investigations and reviews where there would be an expectation that more independent and transparent oversight is required. That is the very reason why Attorney General Ashcroft expanded the OIG's jurisdiction in 2001 to include the FBI and the DEA, and there simply is no reason why Department attorneys continue to be protected from the possibility that their conduct may warrant independent review by the OIG in appropriate cases.

Monitoring Department Contracts and Grants

As the Department strives to address some of the nation's most serious domestic and international threats, it must also do so in a fiscally responsible way. From FY 2005 to FY 2015, Department annual spending on contracts increased from $4.5 billion to $7.8 billion, while grants decreased from $5.8 billion to $3.8 billion during the same period. Recently, however, Department spending on grants has increased significantly. For example, between FY 2014 and FY 2015, Department grant spending grew by over $1.5 billion, due in large part to an increase in grant awards under the Crime Victims Fund (CVF), discussed below. Grant and contract funds are spent to help accomplish goals as varied as reducing crime, housing prisoners, and providing services to victims and at-risk populations. As stewards of taxpayer funds, the Department must act responsibly and wisely in managing these resources.



Source: Federal Procurement Data System and USASpending.gov

The Department faces significant challenges in ensuring effective oversight of its contracts and grants. In FY 2016, OIG's audits revealed nearly $25 million in questioned costs and reported over $2 million in funds that should have been put to better use, with 353 recommendations for management improvement. Additionally, the OIG's work has recently resulted in the recovery of nearly $5 million in money paid to contractor employees or credited back to the Department to address audit findings. While the Department's grant-making components have improved their oversight of grantees over the past several years, as referenced below, this remains a continuing challenge, especially since contract and grant spending represents a large a slice of the Department's $37.9 billion FY 2016 discretionary and mandatory budget.

Spending on Contracts

The Department awards contracts to procure a range of goods and services, from basic office supplies to aircraft operations. Given the increase in the amount of Department funds awarded to contractors over the past decade, the OIG has become increasingly involved in auditing contracts. In that role, we have observed significant challenges in both the Department's awarding and its monitoring of contract funds.

To effectively use the contracting process, the Department must comply with federal regulations by determining its needs prior to solicitation and then fully evaluating all bids prior to award. Our recent audit work has identified instances in which the Department failed to follow procedures designed to ensure fiscal responsibility and basic fairness in these processes. For example, in an audit of two FBI fuel procurement contracts, we found that the FBI did not award a bulk fuel procurement through the FAR-identified mandatory source and did not establish a requirement for the specific fuel type for the Miami Field Office. Similarly, our audit of DEA's Aviation Operations with the Department of Defense in Afghanistan found that the DEA did not fully comply with the Federal Acquisition Regulations (FAR) and its own solicitation in purchasing an aircraft for over $8 million.

Source: OIG

The Department also faces challenges monitoring contracts after monies have been awarded. Monitoring a contract post-award helps ensure the contractor abides by its terms, including those that govern the proper use of funds, compliance with laws and regulations, and contractor performance to achieve anticipated outcomes. Again, our audit of the DEA's Aviation Operations in Afghanistan showed major deficiencies in these areas. We found that the program had missed every intended delivery date from the first delivery date in December 2012. Those missed deadlines contributed to the program cost spiraling to $86 million, almost four times the original anticipated amount of $22 million, and the aircraft was still not operational as of June 2016.

The OIG recently identified similar challenges in how the BOP monitors contract prisons. In an August 2016 report, we found that the BOP still had monitoring improvements to make since our 2015 audit of the Reeves County contract prison, discussed in last year's report. We found that a checklist in the BOP's Quality Assurance Plan did not address certain important BOP policy and contract requirements in the areas of health and correctional services. As a result, the BOP has not been able to effectively ensure that contract prisons comply with these requirements. The week after our audit was released, the Department announced that it would begin the process of reducing and ultimately ending its use of privately operated prisons.

Spending on Grants

Grant funding also presents challenges, as the Department must not only guard against fraud and mismanagement but also seek to enhance taxpayer value by finding ways to better measure and ensure positive outcomes. As with contracts, our recent OIG work has identified challenges in both allocation and oversight of these expenditures.

In last year's Top Management and Performance Challenges report, we highlighted the enhanced responsibility the Department would face in its management of the CVF due to the over three-fold increase in the amount of CVF funds Congress authorized the Department to spend in FY 2015. In FY 2016, Congress increased the cap on CVF spending by over $600 million to more than $3 billion, most of which OJP's Office for Victims of Crime distributes via grants to programs intended to assist victims of crime. Rather than tax dollars, the CVF is financed by fines and penalties paid by convicted federal offenders. Nonetheless, an increase in available funds brings with it an increased risk of misuse and mismanagement. To monitor increased CVF spending, the OIG was allocated $10 million from the CVF in both FY 2015 and FY 2016 for enhanced oversight and auditing activities related to the fund. We are currently conducting a risk assessment of OJP's management of the CVF.

Simultaneously, the OIG continues to conduct audits of state CVF formula grantees and their allocation and management of funds to sub-grantees to ensure adherence to the terms of the grants. In these audits, we have identified various areas in need of improvement, including instances in which grantees failed to properly monitor sub-grantees. For example, in a recent audit of ten CVF formula grants, the OIG found that the California Governor's Office of Emergency Services was funding several sub-grantees with histories of fraudulent and even criminal conduct, while also failing to issue sub-recipient monitoring reports in a timely manner.

In addition to challenges in grant allocation, the Department must also ensure proper post-award oversight. OIG work has identified instances in which the Department was unable to ensure adequate performance by grantees and sub-grantees. Some examples include the failure by grantees to comply with essential grant conditions; maintain adequate records and accounting systems; and submit accurate, complete, and timely financial and performance reports.

Such challenges were highlighted in a November 2015 audit of an OVW grant to the Dawson County Domestic Violence Program in Glendive, Montana. In that audit, we questioned the entire amount—nearly $4 million—the grantee had used because the grantee was unable to provide a complete and accurate set of accounting records. In addition, limitations in the grantee's tracking system inhibited the OIG from adequately assessing program performance and, thus, taxpayer value. For example, the grantee could not even confirm the total number of victims served.

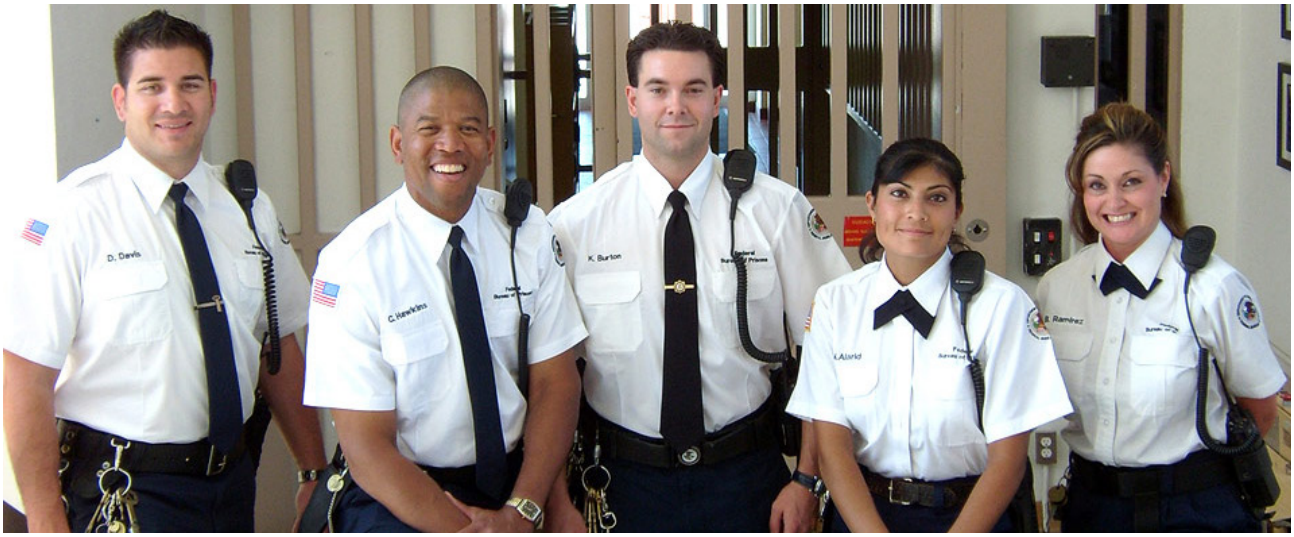
The OIG continues to work with the Department's grant-making components to ensure that grant dollars are used to achieve positive outcomes. For example, in 2015, we conducted an audit of grants awarded to the Navajo Division of Public Safety through OJP's former Correctional Systems and Correctional Alternatives on Tribal Lands Program. We found that the grantee constructed two correctional facilities with capacities that were at least 250 percent larger than needed. Since the completion of our audit, one facility has not yet opened due to construction issues, and the other facility is 82-percent vacant. The OIG is continuing to monitor open recommendations from the audit and is also conducting a comprehensive audit of OJP's management and oversight of the Tribal Justice Systems Infrastructure Program (formerly the Correctional Systems and Correctional Alternatives on Tribal Lands Program).

At recent Congressional hearings, top officials within OJP spelled out steps they are taking to improve OJP's processes. These steps include (a) collaborating with other components to prevent duplication of efforts, (b) establishing procedures to identify and monitor high-risk grantees, (c) providing enhanced technical assistance to grantees, and (d) verifying grantee claims of program success by collecting and examining source documentation.

The OIG's work illustrates that the Department must improve its oversight of its contract and grant award and monitoring efforts to guard against waste, fraud, abuse, and mismanagement, and to ensure the most efficient and effective use of taxpayer funds.

Managing Human Capital and Promoting Diversity With a Workforce Increasingly Eligible to Retire

Agencies across the federal government face the challenge of hiring and retaining talented employees with the skillsets needed to accomplish agency missions, while their aging workforces increasingly become eligible to retire. This challenge represents a serious problem for the Department—and the public that it serves and protects—if it is unable to hire and retain experienced agents and attorneys with the specialized skills needed to investigate and prosecute complex cases related to, for example, terrorism, cybersecurity, financial crime, civil rights, and public corruption. As of September 2014, approximately 31 percent of the Department's permanent career employees were eligible to retire by 2019. In the next 10 years, 85 percent of the federal government's Senior Executive Service will be eligible to retire. As the number of retirement-eligible employees grows, the Department needs to develop long-term strategies to recruit and retain a skilled and diverse workforce.



Source: BOP website

Managing Human Capital To Prepare For Increasing Numbers of Retirements

Succession planning in the government offers unique challenges for agency leaders. From FYs 2005 to 2014, retirement in the Executive Branch increased by 10.9 percent. During this time, mandatory retirements also increased by 83.8 percent. As the rate of federal retirements continues to increase, the Department has an opportunity to institute proactive policies and guidance that guard against the loss of institutional knowledge and to maintain continuity of operations. In facing this transition in its workforce, the Department must strive to mitigate the loss of institutional knowledge created by the retirements of senior employees and managers, ensure that mid-career employees are prepared to take over senior positions, and train new employees to step into important leadership roles.

A unique challenge for the Department's law enforcement components is the difficulty retaining experienced Special Agents in management positions because agents are eligible for full retirement at age 50 with 20 years of service, and know they must retire at age 57. As a result, experienced agents often retire or take private sector positions well before those in most other federal occupations. Law enforcement leaders in the Department have told us this has a negative impact on the level of experience and knowledge of upper-

management in their ranks. One option that law enforcement components can use in special cases is to grant extensions allowing agents to work past their mandatory retirement age; however, given its limits, this choice is not a solution to the larger problem.

Hiring Quality Candidates to Ensure Department Mission and Agency Goals are Met

As the Department recognizes, its employees are its greatest assets. The Department's challenge is to recruit skilled and diverse talent to help meet mission goals. Advances in technology will continue to affect every aspect of Department operations such as data management, communications, cyber investigations, and cybersecurity. It is therefore imperative that the Department be innovative in its efforts to fill vacant positions that require specialized skills, in areas such as Science, Technology, Engineering, and Mathematics (STEM). As we note in the section on Cybersecurity, the FBI faces significant challenges in hiring qualified IT experts to address its responsibilities in this area given competition from the private sector. These challenges have grown even more acute as some segments of the economy have experienced economic growth and IT job vacancies outnumber those who can fill them.

Another example of the challenge in hiring experts with a STEM background is the Department's difficulty hiring medical professionals for its federal correctional institutions. In March 2016, the OIG conducted a review of the BOP's medical staffing challenges and found that multiple factors, including pay, the location of the institutions, and the correctional setting itself, negatively impact the BOP's ability to recruit and retain medical professionals. The OIG also found that the salaries and incentives the BOP offers are not competitive with those of the private sector, particularly given the need to compensate BOP employees for working in a correctional setting.

Source: DOJ

Another hiring challenge for the Department in recent years has been adjusting to the generational shift in the workforce. For example, in 2006, nearly 47 percent of the Department's workforce was under the age of 40, while only 9 percent of Department employees were 55 and older. Ten years later, Justice Management Division (JMD) data shows that approximately 24 percent of the Department's workforce is age 35 and under (often referred to as "Millennials"), 52 percent are ages 36 to 51 (often referred to as "Generation X"), and 24 percent are age 52 and older (often referred to as "Baby Boomers"). While the Department's workforce is aging, it must address the additional challenge of generational changes as it seeks to bring on board younger employees. The President has recognized that students and recent graduates "infuse the workplace with their enthusiasm, talents, and unique perspectives." OPM has found that one of the best ways to ensure the federal workforce better reflects the people it serves is to actively recruit the next generation of federal employees. However, while the workforce is trending younger, the traditional federal hiring process still favors applicants possessing prior work experience. To meet this challenge, the Pathways program, which recruits students and recent graduates with less work experience, has evidence of being effective. Using Pathways, the Department hired 170 employees in FY 2015 and 113 employees FY 2016. Moreover, OPM statistics show that 93 percent of those hired through Pathways want to stay in government. This program has the potential to help mitigate the impact of increasing retirements by bringing on board a new generation of talented employees who can begin developing institutional knowledge at the outset of their careers, and potentially develop into future leaders.

OPM has also found that offering telework to employees is an important recruitment and retention tool, and it helps to improve employee attitude and job satisfaction across the federal workforce. However, the Department's current telework participation rate is 11 percent, far below the government-wide participation rate of 31 percent. While we recognize that telework opportunities for those with law enforcement responsibilities are more limited, we nevertheless believe that a participation rate of only 11 percent suggests there is opportunity for improvement in this area.

Once a new employee has been selected, it is critical for the Department to make the hiring process as swift as possible, particularly for positions deemed mission critical. OPM has set 80 days as the goal for federal agencies to complete the hiring process. While this is a useful target, we recognize it might not be practical for agencies such as the Department that have unique hiring needs. Still, JMD statistics suggest there is room for improvement, as they show that on average it took more than 5 months to hire attorneys (225 days), criminal investigators (162 days), IT specialists (190 days) and legal assistants (248 days)—all deemed mission critical positions. The Department's FY 2014-2018 Strategic Plan sets a goal to evaluate a new system that would enable human resources staff to hire people faster by automating manual and paper-based processes. Another significant factor delaying employee start dates can be the time required to complete background checks, which need to be performed in a timely manner. In 2012, the OIG released a report finding that clearances for mission critical positions in the Department such as agents, intelligence analysts, and linguists, consistently took longer than 60 days, a benchmark that agencies are expected to achieve 90 percent of the time under the *Intelligence Reform and Terrorism Prevention Act of 2004*.

Retaining Diverse Talent to Minimize the High Cost of Employee Turnover

The Department must also focus on retaining the talent it hires in order to hold down high turnover costs. OPM estimates turnover costs can range from 90 percent to 200 percent of an employee's annual salary. The Department should consider how programs that encourage diversity, mentorship, employee engagement, and accountability between managers and those they supervise, can improve workplace environments and foster retention.

Source: DEA website

Establishing a diverse work force is a challenge for the Department across the organization, but particularly at the management level. Data shows only 35 percent of employees at the GS-14 level and above are women, and only 23 percent are from racial and ethnic minority groups. While announcing a new report promoting diversity in law enforcement, in October 2016 Deputy Attorney General Yates noted the benefits of having police "reflect the communities they serve." A growing body of evidence suggests diversity can make policing more effective, safe, and just, according to the report by the Civil Rights Division and the Equal Employment Opportunity Commission. Although the report was focused on local law enforcement, it offered advice on recruitment, hiring, and retention that could be of value to the Department's own law enforcement components. Statistics show that as of FY 2014, 69 percent of the Department's criminal investigators were white men, 12 percent were white women, 15 percent were minority men, and 3 percent were minority women.

Engaging employees is one way to improve retention. The Department can accomplish this by providing ways for employees to enhance their skillsets. Another method encouraged by OPM is that employees have multiple mentors in different areas, such as a career guide, an information source within the office to help an employee understand how the office works, a friend to confide in, and an intellectual guide. Employee

engagement can also be improved by creating developmental assignments for employees to grow their abilities, and ensuring that employees are cross-trained in order to preserve institutional knowledge that might be lost with an employee's retirement or extended absence. Interestingly, the 2015 Federal Employee Viewpoint Survey (FEVS) found that although 68 percent of Department respondents were satisfied with employee engagement, only 58 percent were satisfied with how agency leaders communicate with and motivate their employees.

Another challenge for the Department is to ensure that managers and employees are held accountable for their performance. According to OPM, a bad hire can cost an agency as much as three times an employee's salary. To illustrate, if an agency hires a GS-14 or GS-15 employee who is not fully successful during the probationary period, it could cost the agency more than $300,000. According to the 2015 FEVS Survey, 44 percent of respondents did not think Department managers were taking sufficient steps to deal with poor performers who either cannot or will not improve. However, managers point out that often co-workers are unaware that actions are being taken to address poor performance because the *Privacy Act* places limits on what managers can disclose about disciplinary actions they take.

The Department will continue to face challenges as an increasing number of employees retire and take with them a vast amount of institutional knowledge. The Department must ensure that it responds to this generational shift by recruiting and retaining a diverse workforce with varied skillsets. To do so, the Department will need to look for innovative strategies and improve on-boarding time, among other things, to remain competitive with other markets and attract the most qualified candidates for critical Department operations.

Using Performance-Based Management To Improve DOJ Programs

A Challenge Facing Every Component and Program

In an era when government agencies at the local, state, and federal level are moving toward a more widespread recognition of the importance of a data-driven approach to planning and management, our reviews have repeatedly found that this remains a significant challenge for the Department. From the Department's failure to evaluate "big data" on important criminal justice issues, such as whether its detention and rehabilitation programs impact recidivism, or knowing how many officer-involved shootings there have been across the nation, more needs to be done. While this challenge appears at the end of this report, it does so precisely because it impacts every one of the challenges previously discussed, illustrating how the deficit in performance-based management is a challenge across many of the Department's programs.

For example, the Department's primary method of measuring crime in the United States remains the FBI's 1930s-era annual compilation of Uniform Crime Reporting (UCR) statistics. Yet, as the FBI has acknowledged, these crime statistics do not sufficiently characterize crime today (they do not, for example, explicitly address cybercrime), and are far less useful in directing enforcement efforts than they otherwise could be if they were available much sooner, instead of nine months after the previous reporting year ended. Meanwhile, only a third of the nation's law enforcement agencies are reporting crime data using the National Incident-Based Reporting System (NIBRS), a much more comprehensive system the FBI developed in 1989 to replace the UCR's summary reporting. Although the FBI, working with the Bureau of Justice Statistics, is committed over the next four years to try and recruit a statistically-representative sample of law enforcement agencies to use NIBRS, and has transferred $45 million to BJS so far to support this work, a more comprehensive crime data solution appears years away.

Source: FBI website

At a time when some big city police departments can tell you where and when every gunshot was fired in the city with audio recordings of the shots e-mailed instantly to precinct captains' cell phones with precise geo-location information, the Department has much it can learn from its local law enforcement partners. Because police departments in some cases have detailed crime data available in near real-time, federal prosecutors are working with them to gather the information they need to figure out where to focus limited federal resources to fight gang and gun violence. Although these partnerships hold much promise for future federal, state, and local law enforcement collaboration, they illustrate that when it comes to crime data, the Department is often playing catch up with its local counterparts. Not having a national database of accurate information on shootings, including police shootings, is just one symptom of the lack of timely and comprehensive crime data. Without such information Department officials are stuck trying to tackle a problem they cannot accurately measure or analyze.

At the other end of the criminal justice process, the BOP has not released statistics on the recidivism rate of federal prisoners in more than 20 years. So although the BOP spent $7.8 billion in FY 2016 to cover inmate needs such as housing for nearly 200,000 federal prisoners, the Department cannot determine with much accuracy whether its prison system is achieving the twin goals of deterrence and rehabilitation. As discussed in the Prisons challenge, our August 2016 review of the BOP's RPP found that, "the BOP does not collect

comprehensive re-arrest data on its former inmates, has no performance metrics to gauge the RPP's impact on recidivism, and does not make any attempt to link its RPP efforts to recidivism." Similarly, the BOP spent roughly $360 million a year in FYs 2014 and 2015 on approximately 200 Residential Reentry Centers, but it does not currently track the success of its RRC programs, a subject of one of our ongoing BOP reviews. On a positive note, the BOP has announced its intention, as part of its strategic plan, to use data to begin monitoring the success of various RRCs beginning this summer. It needs to do so to tap into the potentially vast laboratory of innovation available to make its programs as efficient and effective as possible.

Multiple mandates affirm the importance of performance-based management. For example, OMB Circular A-11 requires agencies to conduct at least quarterly, data-driven performance reviews on their organization's priorities to drive progress toward achieving their goals. OMB Circular A-11 describes this approach as a "management practice proven to produce better results." Similarly, the *Government Performance and Results Modernization Act of 2010* (GPRAMA) requires agencies to engage in performance management tasks such as setting strategic plans or completing annual performance plans. Additionally, the *Digital Accountability and Transparency Act of 2014* (DATA Act) directs the federal government to transform all spending information into standardized, easy-to-read data formats for better transparency. Implementation of the DATA Act will not only expand the information available to the public, but will also give the Department access to that information in a standard data format for use in management and decision making. A September 2015 GAO report found that, "if fully and effectively implemented" the DATA Act and GPRAMA could allow executive branch agencies and Congress to accurately measure the costs and magnitude of federal investments.

Collecting The Right Data

The challenge for the Department with all of its programs is to ask, "Are we collecting the right information?" However, simply collecting data, using metrics, and labeling a process "performance-based management," does not satisfactorily comply with GPRAMA and OMB guidance or the important policies underlying them. The Department must ensure it identifies performance metrics to adequately measure program outputs and must identify and collect the right data to measure its programs' impacts. As mentioned in the Prisons section, a July 2016 OIG audit found that neither the EOUSA nor the USAOs track the total number of participants placed into pretrial diversion programs. The result is an inability to calculate whether the use of such programs is meeting the goals of the Department's Strategic Plan and its Smart on Crime initiative.

Source: DOJ

Ensuring the Department effectively collects data and that the data collected reveals the true story is a challenge that impacts every facet of the Department's operations. For example, the OIG discovered that the BOP uses two systems to track recovered contraband cell phones and that over a 3-year period there was a difference of more than 41 percent in the cell phone contraband data reported between the two methods. The BOP's data collection methods, coupled with the lack of established guidance and policy on accurately and consistently documenting recovered contraband, impede its ability to effectively track contraband recoveries and analyze contraband trends. Without a reliable method to ascertain the true amount of contraband and the efficacy of its interdiction efforts, the BOP cannot fully address questions regarding prison safety.

Additionally, the Department needs to be vigilant to ensure that its data collection and metrics are accurately being used to measure program performance. For example, the OIG's audit of the FBI's Regional Computer Forensic Laboratory (RCFL) discovered that, as a result of the FBI changing its "definition" of what constituted a backlog, what appeared to be a decline in the backlog at the RCFL in fact reflected a continuing backlog. This is similar to the double counting of total cases opened by immigration courts that we noted in our 2012 review of the Management of Immigration Cases and Appeals by the Executive Office for Immigration Review (EOIR). We also found in that review that EOIR's performance reporting data underreported actual processing time, which undermined EOIR's ability to identify appeal processing problems and take corrective action. Only by choosing appropriate measures and accurately reporting on them can the Department ensure that its use of metrics will help improve Department programs. This is the essence of performance-based management and it remains a challenge for the Department.

Verifying The Data Collected Is Accurate and Reliable

Another challenge in performance-based management is verifying that the data collected is valid, accurate, and reliable. As we have included in past TMPC reports, our work has found numerous instances where data was inaccurate, unreliable, or unsupported. There are more instances of such findings from this year as well. As mentioned in the Contracts section, the OIG questioned nearly $4 million in a November 2015 audit of an OVW grant where the grantee could not confirm the total number of victims served or provide information that would allow the OIG to assess the program's performance. Our April 2016 audit of the OVW grants awarded to the Native Women's Society of the Great Plains, in Eagle Butte, South Dakota, found that the grantee could not provide adequate documentation to support the activities recorded in its progress reports.


Source: OIG

However, data reliability is not just an issue with grantees, but is an area in which the Department can improve as well. For example, our March 2016 audit of BOP's Armory Munitions and Equipment found weaknesses in BOP's controls over tracking, issuing, and reporting on both active and expired armory munitions and equipment. This inaccurate data increases the risk that armory munitions and equipment could be lost, misplaced, or stolen without being detected. Further, our March 2016 audit of the National Institute of Justice's Management and Oversight of DNA Backlog Reduction Grantees' Reporting and Use of Program Income emphasized the need for the Department to provide clear direction to grantees so the data it receives is reliable. In that audit, we found that important calculations of program income were often incorrect because the grantees had not received proper training on the calculation tool provided by the NIJ. As a result, the grantees submitted inaccurate program income calculations and reporting. In order to fully implement performance-based management, the Department must ensure that it provides guidance to those submitting data to ensure that the data provided is valid, accurate, and reliable prior to its analysis and use by the Department in program management decisions.

Analyzing The Data Collected

Another challenge for the Department is to collect and analyze data showing program results, and more significantly, *program impact*. Analyzing Department program data in meaningful ways to determine impact is essential to managing the effectiveness of these programs going forward. For example, we found in our review of the BOP's Medical Staffing Challenges that the BOP tracks the use of incentives only to ensure that spending remains within budgetary limits and not to identify the hardest to fill vacancies in the BOP system. Analyzing data to determine the hardest to fill vacancies could assist the BOP in more effectively managing its workforce, which in turn is essential to fulfilling its mission.

Such performance analysis is critically important, both when it shows program success and when it indicates that a program is falling short of its goals. In our February 2016 audit of the DEA's Controls Over Seized and Collected Drugs, for example, we found that DEA personnel still sometimes failed to meet inventory management requirements despite the increased time allowed for its personnel to complete tasks. The delayed entry of drug exhibits increases the risk of evidence tampering, misplacement, or loss, which in turn impacts the effectiveness of the DEA's program. Program management in such instances should analyze performance metrics to inform necessary program changes to eliminate problem areas and thereby increase the effectiveness of the Department's programs.

Furthermore, Department components should review what has and has not worked for other components to effectively leverage knowledge from past efforts. For example, in our February 2016 review of Department and ATF's implementation of recommendations contained in an earlier Fast and Furious report, we found several areas where the Department and ATF improved their ability to assess risk metrics in law enforcement operations but also discovered that performance-based lessons learned from one Department component's performance issues are not adequately evaluated and integrated by other components. Such disparities reflect the need for Department leaders to be engaged in making sure reforms made in one component are considered by their fellow components, so each can learn from the others.

The performance-based management challenge is more than a standalone challenge—it permeates all of the other Department challenges. From creating a comprehensive crime data solution to the analysis of BOP data to determine the recidivism rate of federal prisoners released to the public, the collection and analysis of performance measures is essential to effectively and efficiently managing Department resources to ensure that its programs consistently achieve the greatest possible impact on the many difficult challenges it faces.