OIG Top Management and Performance Challenges Facing the Department of Justice – 2018

October 15, 2018

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 2018 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:

- *Advancing National Security, Protecting Sensitive Information, and Safeguarding Civil Liberties*
- *Enhancing Cybersecurity with Emerging Technology and Collaboration*
- *Managing an Overcrowded Federal Prison System in an Era of Declining Resources*
- *Building Productive Relationships and Trust Between Law Enforcement and Communities*
- *Coordinating within the Department and Across Government to Fulfill the Department's Mission to Combat Crime*
- *Administering and Overseeing Contracts and Grants*
- *Effectively Applying Performance-Based Management to Inform Decision Making and Improve Outcomes*
- *Filling Mission Critical Positions Despite Department Challenges and Delays in the Onboarding Process*
- *Ensuring Adherence to Established Department Policies and Procedures*

This year, eight of the nine challenges are issues the OIG identified in last year's memorandum. For the first eight challenges in the list above, we discuss the Department's progress in meeting the challenges and also discuss new and ongoing areas of concern. A persistent theme throughout the challenges we identified is the threats caused by emerging technologies -- from the development and distribution of synthetic opioids, to increasingly sophisticated cyber-attacks, to drone technologies that threaten the physical security of federal prisons. For each emerging technology, the Department must have a workforce capable of responding to the threat, and the ability to recruit and retain professionals in each of

these fields creates its own challenge for the Department. The new challenge identified in this year's memorandum is an ongoing concern, but one that was highlighted persistently in the OIG's work this year. This is the need for all Department employees to adhere to established policies and procedures. As noted in recent OIG reviews, the actions of a few, especially individuals in leadership positions, can undermine the Department's reputation for professionalism, impartiality, and fairness when policies and procedures are not consistently followed.

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.

ADVANCING NATIONAL SECURITY, PROTECTING SENSITIVE INFORMATION, AND SAFEGUARDING CIVIL LIBERTIES

In Fiscal Year (FY) 2019, the Department's primary strategic goal is to enhance national security and counter the threat of terrorism. With a threat environment that is constantly evolving, the Department must balance the use of new technology with legal authorities to ensure the protection of privacy and civil liberties for American citizens.

Combatting Foreign and Domestic Terrorism

One of the Department's highest priorities is combatting foreign and domestic terrorism, which threaten our national security and the safety of the American public. The Federal Bureau of Investigation (FBI) leads the Department's counterterrorism efforts and, in FY 2017, dedicated over 5,000 full time employees and more than $1 billion to this key mission area. Currently, the FBI views the Islamic State of Iraq and Syria (ISIS) and Homegrown Violent Extremists (HVE) as the main terrorism threats to the United States. Due to technological advances, the message of radicalization continues to spread in ways previously unimagined. In recognition of this continuing threat, the OIG is conducting an audit of the FBI's efforts to address HVEs, which includes evaluating the FBI's policies and procedures used to identify and investigate these threats. Additionally, the OIG is conducting an audit of the Bureau of Prisons' (BOP) efforts to monitor communications of inmates with known and potential ties to domestic and foreign terrorism, as well as its efforts to prevent radicalization among its inmate population.

Management Advisory Memorandum (MAM) Concerning Homegrown Violent Extremism

In June 2018, the OIG issued a MAM to the FBI Director regarding a threat to national security, stemming from a HVE, operating from a federal facility, outside of DOJ's authority. FBI management took formal steps to coordinate with the non-DOJ federal entity to address the identified concerns. The MAM made five recommendations to the FBI.

The Department shares responsibility with the Department of Homeland Security (DHS) in leading federal efforts to counter violent extremism (CVE) and co-leads the CVE Task Force. However, the Government Accountability Office's (GAO) April 2017 report on countering violent extremism determined that the CVE Task Force has not established a process for assessing whether the federal government's CVE efforts are working. Additionally, in recognition of the importance of cooperation between the Department and DHS on counterterrorism, the OIG is conducting an audit of the FBI's efforts to protect the nation's seaports and maritime activity, including the FBI's assessment of terror threats and coordination with DHS.

Last year, the OIG completed a joint review with the DHS Office of Inspector General and the Intelligence Community (IC) Inspector General on the Domestic Sharing of Counterterrorism Information. The review resulted in 23 recommendations, 11 involving the Department and the FBI, to improve coordination with DHS and the other IC agencies. The report recommended that the Department and FBI evaluate their current processes for sharing counterterrorism information and update these processes to increase collaboration and coordination with other partners. As of August 2018, the OIG has closed 7 of the 11 recommendations, noting that the Department continues to develop a comprehensive counterterrorism sharing strategic plan and that the FBI has taken steps to improve the sharing of counterterrorism information.

Counterintelligence and Counterespionage

Deterring and defeating our adversaries' intelligence and espionage efforts remains a top priority for the Department. In a 2017 statement to the House Homeland Security Committee, FBI Director Christopher Wray warned that "foreign intelligence services and other state-directed actors continue to employ more creative and more sophisticated methods to steal innovative technology, critical research and development data, and intellectual property, in an effort to erode America's economic leading edge." In addition to threats to our economy, foreign actors have initiated attacks intended to disrupt U.S. democratic institutions, including our elections. Assaults on our economic and political institutions often utilize sophisticated technology. Combatting this threat is a top priority for the Department. In November 2017, to better coordinate the Department's efforts to counter the threat of harmful foreign influence, the FBI established the Foreign Influence Task Force (FITF), which integrates the FBI's cyber, criminal law enforcement, counterterrorism, and counterintelligence resources to serve as the central coordinating authority for investigations involving foreign influence operations. For further details regarding the Department's efforts to neutralize and defeat cyber-attacks, see the *Cybersecurity* section of this report.

The Foreign Agents Registration Act (FARA) is another counterintelligence and counterespionage tool that helps identify individuals acting as agents of foreign principals within the United States. In its September 2016 report on the National Security Division's (NSD) administration and enforcement of FARA, the OIG found inconsistent interpretations of the law between agencies, leading to minimal criminal enforcement between 1966 and 2015. As of August 2018, the Department had addressed all 14 report recommendations, including those that recommended the Department develop a comprehensive strategy to integrate NSD's FARA compliance and enforcement work with the Department's overall national security strategy.

Insider Threats: Preventing the Unauthorized Disclosure of Sensitive Information

Source: FBI

Insider threats remain a serious concern across all of government. Employees who misuse or betray, wittingly or unwittingly, their access to any U.S. Government resource can cause catastrophic damage to the operational security of the Department and the nation. Insider threats pose a significant risk because they can disclose highly sensitive information directly to unauthorized, non-government sources, allowing for fast, global consumption of leaked information. Ensuring effective personnel security is one measure that can prevent and deter insider threats.

A September 2017 OIG report on the FBI's Insider Threat Program highlighted several areas in which the FBI can better deter, detect, and mitigate insider threats. The public summary of the classified report contained 8 recommendations to enhance the effectiveness of the program. For example, to improve systems accountability, the OIG recommended that the FBI conduct a comprehensive inventory of classified networks, systems, applications, and other information technology assets and identify a component responsible for maintaining the inventory. The FBI concurred with the OIG's recommendations and has implemented 2 of them to date, including a recommendation that the FBI notify the OIG of all insider threat investigations, including threats classified as counterespionage, in a timely manner, consistent with the Inspector General Act and Department regulations. Additionally, in response to recent unauthorized disclosures of sensitive information, the FBI established a unit within the Counterintelligence Division to oversee and manage investigations of leaks of classified information.

Polygraph examination is an additional tool used by the FBI to detect potential security threats among employees and prospective employees expected to have access to national security information. In a March 2018 report, the OIG found that the FBI's process for responding to unresolved issues in polygraph examination results may lead to both security and operational vulnerabilities. The OIG issued 8 recommendations to assist the FBI in improving its processes to enhance the utility of its polygraph program.

Leveraging National Security Legal Authorities While Safeguarding Civil Liberties

The Department faces continuing challenges in safeguarding the civil liberties of U.S. citizens and residents while using existing legal authorities to combat terrorism and espionage, as well as conduct its counterintelligence mission. One such challenge involves assuring Congress and the American public that the privacy safeguards built into Section 702 of the *Foreign Intelligence Surveillance Act* (FISA) *Amendments Act* are effective.

In response to requests from Attorney General Sessions and Members of Congress, as well as in furtherance of its oversight mission, the OIG is currently examining the Department's and the FBI's compliance with legal requirements, policies, and procedures in applications filed with the U.S. Foreign Intelligence Surveillance Court relating to a certain U.S. person.

Other challenges are presented by fast evolving technology, developments in law relating to personal data now routinely stored, and the public's heightened interest in data security to protect against identity theft and other personal intrusions. For example, recent court decisions have placed greater limitations on the requirements for law enforcement to obtain location information of personal mobile devices. In addition, the Department and the FBI encountered difficulties accessing information stored on the iPhone of the gunman responsible for the December 2015 mass shooting in San Bernardino, California. Although the OIG's March 2018 report relating to that incident (see text box) did not address this issue, it described obstacles encountered by the FBI in its investigation.

OIG Report on the Accuracy of FBI Statements Concerning its Capability to Access Data on an iPhone Seized During the San Bernardino Terror Attack Investigation

The OIG conducted an inquiry into whether FBI officials, including former Director James Comey, made inaccurate statements to Congress or caused inaccurate statements to be filed in court regarding the FBI's ability to access data on an iPhone seized during the investigation of the December 2015 terror attack in San Bernardino, California. The OIG found no evidence that the FBI had the capability to access data on the iPhone at the time of former Director Comey's February and March 2016 congressional testimony or the February 2016 initial court filing requesting involuntary assistance from Apple, Inc. to access the phone. Therefore, we determined that the testimony and initial court filing were not inaccurate when made.

The Department faces growing challenges in obtaining electronically stored information necessary to fight crime and protect the national security when individuals' demand for privacy is growing and corporate efforts to satisfy that demand are becoming more sophisticated.

ENHANCING CYBERSECURITY WITH EMERGING TECHNOLOGY AND COLLABORATION

In July 2018 remarks at the Aspen Security Forum, Deputy Attorney General Rod Rosenstein stated that "the digital infrastructure that serves this country is literally under attack." The Department has taken a number of steps to respond to these attacks on the country's digital infrastructure and to develop a comprehensive cybersecurity strategy. For example, in February of 2018, in response to cyber-attacks and other threats posed by hostile foreign actors targeting institutions, Attorney General Sessions established the Cyber-Digital Task Force, with the goal of determining how the Department can more effectively respond to global threats. The Cyber-Digital Task Force report, issued in July of 2018, outlines the following cybersecurity challenges facing the Department of Justice: (1) preventing and responding to cyber incidents; (2) investigating and prosecuting cyber-related crimes; and (3) dismantling, disrupting, and deterring malicious cyber threats.

The Evolving Threat of Cyber Intrusions

Protecting the nation against cyber-based attacks, both foreign and domestic, continues to be one of the Department's top goals. To be fully prepared to respond to the emerging and evolving threats from cyber-attacks, the Department must continue to update its strategies, recruit and retain a dynamic workforce as discussed in more detail in the *Human Capital* section of this report, and ensure that internal systems are secure.

Source: FBI

Cyber intrusions and attacks can undermine advantages held by the U.S. military and result in national security breaches, economic losses, failures in critical infrastructure, and intellectual property theft. Since at least March 2016, foreign government cyber actors have targeted government entities and multiple U.S. critical infrastructure sectors including energy, commercial facilities, water, aviation, nuclear, and critical manufacturing. Computer intrusions, such as spear phishing, are increasing in number and sophistication. Therefore, the Department must keep pace with evolving technologies to protect American interests.

Alongside the more traditional, physical infrastructure and information targets, malign foreign actors have also begun using cyber-attacks to incite societal discourse for geopolitically motivated objectives. By routing their activities through complex computer networks across the globe and using crypto-currency (including bitcoin), these actions were difficult to track and attribute.

To best confront these challenges, and ensure that resources are directed to the most significant cyber threats, the FBI must implement an objective, data driven approach to its prioritization of cyber threats and cases. As noted in a 2016 OIG audit, the current cyber prioritization process is subjective and not updated frequently enough to be fully effective. While the FBI agreed with the OIG's 2016 recommendation to improve the cyber threat prioritization process, the recommendation remains open.

The Department also must continue to take steps to ensure its own information systems are secure. In the OIG's FY 2017 Federal Information Security Modernization Act (FISMA) audit, the OIG reviewed the information security programs of six Department components and a sample of 14 systems within these components. Recommendations were made in several key areas, including risk and configuration management, identity and access management, and security training, to better enhance the DOJ's information security program. Additionally, to increase transparency and promote accountability in the Department's information security efforts, the OIG now publicly posts the commentary and summary portions of its FISMA reports.

Private Sector Partnerships in Cybersecurity

According to the National Institute of Standards and Technology's National Vulnerability Database, which is sponsored by DHS's National Cyber Security Division, there have been over 107,497 known cybersecurity vulnerabilities and exposures identified by the public and private sectors as of September 2018. These growing threats affect the government and private sector alike. The OIG is currently evaluating the FBI's processes and practices for notifying and engaging with victims of cyber intrusions. Successful engagement can help to better protect vital infrastructure and provide sources of information to assist the FBI with countering future threats. The Department must continue to seek cooperation and information sharing opportunities with the private sector to reduce the level and impact of vulnerabilities and mitigate damage.

Given the pace of technological advances and the dramatic increase in cybercrimes, the Department has made the strengthening of partnerships between the public and private sectors a priority in its current Strategic Plan. The FBI has operated its Internet Crimes Complaint Center (IC3) since May 2000 and has received 4,063,933 complaints of suspected Internet-facilitated criminal activity from inception through 2017. In addition, the FBI has facilitated the sharing of cyber-based information with the private sector by implementing (1) the Private Industry Notifications (PIN) and (2) the FBI Liaison Alert System (FLASH) reports. PINs provide unclassified information that will enhance the private sector's awareness of a threat, and FLASH reports contain unclassified technical information collected by the FBI for use by specific private sector partners.

The FBI has also conceded that there are times when it did not share as much information with the private sector as it could. As demonstrated in a cross-cutting audit report issued in December 2017 by several Offices of Inspector General, including the DOJ OIG, on the Cybersecurity Information Sharing Act of 2015, challenges exist in forging partnerships with private industry. This report identified several impediments to private companies' cooperation with the government to address cybercrimes: antitrust and competitive issues; and perceptions of possible negative business and regulatory consequences in such partnerships, including the public's image of law enforcement actions in cyberspace.

Challenges Investigating & Prosecuting Cybercrime

Disrupting and dismantling illicit DarkNet activity is both a priority and a challenge for the Department as enforcing the law in a global and largely anonymous platform is extremely difficult. For example, malicious actors can utilize botnets, which are networks of computers created by malware and controlled remotely without the knowledge of the computer's user. These present both investigative and prosecutorial challenges as they evolve and

Going Dark

"Going Dark" occurs when the government is unable to access or obtain intelligible information in a useable format (including end-to-end encryption). This poses a serious challenge to law enforcement and has been referred to as one of the Department's most significant challenges when trying to collect investigative data.

increase in sophistication faster than the law's ability to adapt to address the threat. Forging successful partnerships with other federal agencies, as well as international law enforcement agencies can have a positive impact on the Department's effort to investigate and prosecute cyber-crimes. For example, following the successful takedowns of Silk Road 2.0 and AlphaBay, many illicit DarkNet users flocked to a new marketplace called Hansa Market. However, due to already established partnerships with Dutch law enforcement, Hansa Market was quickly shut down. The OIG is currently examining the FBI's implementation of its dark web strategy and efforts to disrupt illegal activities.

The Department has identified gaps in legal authorities that create challenges when attempting to prosecute cybercrimes. For example, federal courts disagree on how to interpret key definitions in the *Computer Fraud and Abuse Act* (CFAA) leading to difficulties in prosecuting individuals who misuse computer networks to which they have access. As a result, an insider with authorized access to a computer network who exceeds his or her authorized access to that network by improperly disclosing sensitive information from that network may not be subject to criminal prosecution under the CFAA. For example, in 2015, the Ninth Circuit Court of Appeals vacated a police officer's convictions under the CFAA for providing confidential police information to a private investigator because the court held that the CFAA only covers inappropriate access to information, such as hacking, not misuse of information gained through an individual's abuse of otherwise appropriate access. The OIG has faced similar challenges in its investigations. A recent OIG investigation substantiated that a DEA employee and an employee from the Department of State (DOS) had searched DOS databases for non-official purposes and provided sensitive and restricted information, which is used to process U.S. visa applications, to a retired DEA official. In another investigation, the OIG found that a DEA employee misused the Texas Prescription Drug Monitoring Program database by conducting an inquiry on a DEA Task Force Officer, who is a doctor. Each of these cases was declined for criminal prosecution.

These loopholes continue to create a challenge for the Department's cyber investigators and prosecutors. For instance, the July 2018 report from the Attorney General's Cyber Task Force states that the CFAA does not prohibit the hacking of a voting machine in common situations, because electronic voting machines generally do not meet the CFAA criteria as computers connected to the Internet. According to the August 2018 statement of an Associate Deputy Attorney General, the CFAA needs to be updated to ensure that it continues to deter violations of Americans' privacy and security.

MANAGING AN OVERCROWDED FEDERAL PRISON SYSTEM IN AN ERA OF DECLINING RESOURCES

In its FY 2019 Budget, BOP requested over $7 billion to manage the federal prison system, which is roughly 25 percent of the Department's discretionary budget. While the federal inmate population has been declining in recent years, many BOP institutions remain over their capacity and providing medical care to inmates continues to account for a major portion of BOP's overall spending at nearly $1.18 billion. Further, the Department has said it anticipates a slight prison population increase in FY 2019. Resource limitations, staffing shortages, and aging infrastructure, combined with this possible prison population increase, has the potential to exacerbate BOP's challenges in ensuring that its institutions are safe and secure. BOP facilities currently exceed total capacity by 14 to 24 percent on average, with high security institutions at the top of this range at 24 percent over capacity on average. Moreover, technological advances have created new challenges for BOP to control contraband entering its facilities. Additionally, as recidivism rates remain high, it is critical that BOP better assess and improve its reentry programs in an effort to reduce recidivism.

Operating in an Increasingly Resource-Challenged Environment While Maintaining Physical Security

Staffing and overcrowding present constant challenges for BOP in carrying out its mission to confine offenders in safe, humane, and cost-efficient environments. In 2015, the then-BOP Director testified before Congress that BOP's inmate to staff ratio "remains high at 4.4 to 1." As of July 31, 2018, that ratio had not changed. Additionally, in 2017, the Department instructed BOP to eliminate 5,000 unfilled, unfunded positions. This has raised concerns that this will increase the occasions when institutions need non-corrections BOP staff members to perform correctional officer duties in order to maintain security.

OIG Review: BOP Management of its Female Inmate Population

The OIG recently completed a review of BOP's efforts and capacity to ensure that BOP-wide policies, programs, and decisions adequately address the distinct needs of female inmates. The OIG concluded that BOP has not been strategic in its management of female inmates, and BOP's programming and policies may not fully consider their needs. For example, we found that BOP could not ensure that its correctional institutions adhered to BOP policies pertaining to female inmates and the BOP Central Office branch that serves as BOP's source of expertise on the management of female inmates may not have adequate staffing to fulfill its mission.

As described above, in addition to staffing challenges, overcrowding in prisons continues to be a concern for BOP. Overcrowding can undermine BOP's ability to ensure the care and safety of the inmate population and the safety of BOP staff. To help alleviate overcrowding, BOP plans to build a new high security prison in Roxana, Kentucky and to transfer low security inmates from BOP institutions to private prisons. However, an August 2016 OIG report found that the BOP needed to do a better job of monitoring its private prisons, which incurred more safety and security incidents per capita than comparable BOP institutions.

Aging facilities and emerging technologies are two additional concerns for BOP in its effort to maintain physical security of its institutions while coping with resource challenges. BOP noted in its most recent Performance Budget that its deteriorated facilities add to increased risk of escape, inability to lock down cells, and potential violence due to frustration over inadequate living conditions. Currently, close to 30 percent of BOP's 122 institutions are over 50 years old, and 43 percent are over 30 years old. BOP also faces growing security threats caused by contraband entering its facilities through technological

advances such as drones. A 2016 OIG report noted deficiencies related to BOP's contraband tracking capabilities, policies, guidance, and training. Cell phones continue to present BOP with safety and security issues. In 2016, BOP confiscated 5,116 cell phones from inmates and this number is on the rise. BOP is reevaluating its strategy to counter these threats. Specifically, as a result of BOP's efforts, the Federal Aviation Administration has restricted the airspace over 20 U.S. penitentiaries to prohibit drones, which supports BOP's mission to maintain safe and secure facilities for inmates and staff. BOP also is currently testing micro-jamming technology to prevent unauthorized wireless communication of inmates and will continue to evaluate cell phone detection technologies to combat this ongoing threat.

Monitoring the Impact of Revised Enforcement Policies on the Federal Prison Population

The Department has announced several new enforcement policies that may result in an increase in the federal prison population. It will be important for the Department to monitor whether the federal prison population, which had decreased over the past several years, increases on account of these polices and to consider the impact of any such population increase on the safety and security on the already over capacity federal prison system.

The Department has announced two new policies regarding immigration prosecutions since 2017. In April 2017, Attorney General Sessions announced a policy that encouraged prosecutors to seek felony charges and pursue mandatory minimum sentences for immigration-related offenses. Further, in April 2018, Attorney General Sessions issued a memorandum that directed each U.S. Attorney's Office along the Southwest border, in consultation with the Department of Homeland Security (DHS), to adopt a zero-tolerance policy for all offenses referred for prosecution. The OIG is currently reviewing the planning and implementation of this policy, and will assess the Department's coordination with DHS and the Department of Health and Human Services on the policy's implementation.

Nearly a quarter of BOP inmates are currently known or suspected aliens, and new immigration enforcement accompanied by revised charging and sentencing policies may increase that number over the coming year. In March 2017, Attorney General Sessions announced the expansion of the Institutional Hearing and Removal Program (IHP) to accelerate criminal alien removal proceedings. The OIG has initiated a review that will examine the IHP expansion efforts, including its coordination with DHS.

The Department's revised charging and sentencing policies may also result in inmate population increases. In May 2017, Attorney General Sessions established a new charging and sentencing policy that directed prosecutors to charge and pursue the most serious, readily provable offenses which carry the most substantial sentences, including mandatory minimums. This new policy effectively rescinded the charging policies and practices outlined in the Department's *Smart on Crime* initiative, which the OIG addressed in a 2017 report. It will be important for the Department to monitor continuously new laws, policies, and initiatives to determine their impact on the already over capacity prison system.

Evaluating the Effectiveness of Efforts to Reduce Inmate Population and Recidivism

In 2016, the United States Sentencing Commission found that nearly half of federal offenders released in 2005 were re-arrested within eight years. Reducing the number of former inmates who return to federal prison is a particularly important task for the Department given BOP institution overcrowding and resource limitations. As a result, the Department is challenged to evaluate the outcomes of programs that seek to decrease the inmate population, through reduced recidivism and other measures, to ensure that they are meeting their established goals. For example, a 2016 OIG audit found that BOP does not have performance measures to evaluate the effectiveness of two incarceration alternatives, Residential Reentry Centers (RRCs) and home confinement, nor procedures that adequately assess services provided by RRC contractors. BOP spends hundreds of millions of dollars annually on reentry programs and RRCs and their contractors, so it is important that the Department be able to measure their effectiveness, especially given its limited resources in this area. A 2017 GAO follow-up report found that the Department had taken initial steps to track outcome data for RRCs and home confinement programs, but that, as of December 2017, the Department had not yet taken steps to measure the outcomes or identify the cost implications of its pretrial diversion programs. A 2018 OIG audit found that BOP has never conducted an evaluation of Community Treatment Services outcomes for inmates in RRCs or under home confinement, does not require contractors to submit performance metrics on its Community Treatment Services program, and does not track the outcomes of the program's stated goals.

Source: BOP

In terms of recidivism, the 2017 GAO report found that the Department has established a plan to evaluate the effectiveness of its reentry programs in BOP facilities. Further, in response to the OIG's 2016 report on BOP's Release Preparation Program, which found that BOP has no performance metrics to determine whether its Release Preparation Programs are successful, BOP stated that it planned to start using statistical analysis to evaluate whether inmates gain relevant skills and knowledge from the program to prepare them for successful reentry to society. However, BOP has yet to conduct the recidivism analysis required by the *Second Chance Act* and, as discussed in past Top Management and Performance Challenges reports, has not published a study on the overall recidivism rate for federal inmates in over 20 years. Further, a 2018 GAO report found that inmates with serious mental illness are more likely to recidivate and recommended that BOP evaluate inmates' recidivism risk and substance abuse and mental health needs to direct treatment to those with the highest recidivism risk. Medical care during incarceration, such as through secure residential mental health treatment programs as described in a 2017 OIG report, represents another avenue for BOP to potentially improve reentry outcomes.

BUILDING PRODUCTIVE RELATIONSHIPS AND TRUST BETWEEN LAW ENFORCEMENT AND COMMUNITIES

The Department plays an important role in fostering trust and building productive relationships between law enforcement agencies and the communities they serve. These relationships are essential to the Department's goal of reducing violent crime and the harm it inflicts on individuals and communities. The Department has a number of available tools and resources that can facilitate law enforcement agencies' collaboration with the communities they serve. The challenge for the Department is effectively using these tools to reduce violent crime while also strengthening police-community relations and ensuring proper oversight of law enforcement officials.

Source: COPS Office

Partnering with Communities to Achieve Violence Reduction and Improve Trust in Police-Community Relationships

The Department's FY 2018-2022 Strategic Plan prioritizes reducing violent crime and emphasizes the importance of partnering with communities to achieve this goal. Law enforcement's efforts to build productive relationships in some communities remains a challenge, strained by law enforcement-involved shootings that increased tensions and mistrust. From 2011 to 2016, the Civil Rights Division's Special Litigation Section, which is responsible for investigating allegations of unconstitutional policing (also referred to as "pattern or practice" violations), logged over 8,600 referrals or complaints that related to state or local law enforcement agencies. In March 2017, Attorney General Sessions announced that the Department was shifting its focus from providing federal oversight of state and local law enforcement practices to local control and accountability for effective policing. The Administration is requesting $140 million in the FY 2019 budget for Project Safe Neighborhoods (PSN), a grant program focused on reducing gang and gun violence, and $5 million for the Public Safety Partnership program (formerly Violence Reduction Network), a technical assistance program that engages communities in developing violent crime reduction strategies. Additionally, as part of PSN, all United States Attorneys' Offices are required to develop violence reduction plans that include robust partnerships with community groups and victims' advocates.

As the Department seeks to reduce violent crime through partnering with communities, recent OIG work has shown that there is room for improvement in the Department's activities aimed at strengthening relations between law enforcement agencies and their communities. In February 2018, the OIG issued an audit report examining the Department's efforts to address patterns or practices of police misconduct and provide technical assistance on accountability reform to police departments. The OIG concluded that the Civil Rights Division (CRT), the Office of Community Oriented Policing Services (COPS Office), the Office of Justice Programs, and the Community Relations Service (CRS) informally coordinated their work, which provided benefits to DOJ's overall efforts in area of police misconduct. However, we found

that more regular and systemic coordination would better enable DOJ components to share information, prevent overlap of services, and ensure efficiency in achieving its goals. The OIG report also found that the COPS Office has not developed a process to assess the effectiveness of its Critical Response program, and the CRS is limited in its coordination efforts with other DOJ components due to a confidentiality provision in its authorizing statute. In another recently issued OIG report, which we discuss in more detail in the *Combatting Violent Crime* section, the OIG identified several deficiencies in the Department's engagement with tribal law enforcement agencies to combat the prevalence of crime in Indian country.

OIG Review: The Bureau of Alcohol, Tobacco, Firearms, and Explosives' (ATF) Implementation of the Frontline Initiative

The OIG is reviewing ATF's implementation of its Frontline Initiative, which launched in 2012. The initiative is ATF's collaborative and intelligence-driven approach to accomplishing its law enforcement and regulatory mission and relies on ATF's partnerships with state and local law enforcement agencies.

Collecting, Analyzing, and Sharing Law Enforcement Data to Enhance Officer Accountability and Safety

The effective collection, analysis, and use of data to improve police-community relations and enhance officer accountability and safety largely depends on the Department's ability to forge longstanding and productive relationships with law enforcement agencies, both within and outside the Department. Despite a recognized need for accurate statistics on use-of-force incidents by law enforcement, the Department has faced several hurdles in gathering and reporting this data. The *Violent Crime Control and Law Enforcement Act of 1994* requires the Department to collect and report data on "the use of excessive force by law enforcement officers," yet the Department has struggled to gather this information as state and local law enforcement agencies are not required to report this data to the federal government and collection methods are inconsistent. Consequently, the Department lacks a national database on police use-of-force incidents that can be analyzed to better inform government decision-makers and the public about the issues raised by law enforcement shootings and develop solutions for reducing them. To address this gap, the FBI plans to add a National Use-of-Force data set to the Uniform Crime Reporting Program that will provide information on police use-of-force that results in a fatality, serious bodily injury, or when a firearm is discharged at or in the direction of a person. Upon approval from OMB, the FBI intends to begin nationwide data collection via a web application. Given that there are more than 18,000 law enforcement agencies across the country and submission of this data remains voluntary, it is particularly important for the Department to exercise leadership and build partnerships with law enforcement agencies if it is to successfully create a comprehensive national use-of-force database that contains accurate, reliable, and timely information.

OIG Review: Death in Custody Reporting Act

The Death in Custody Reporting Act of 2013 requires federal and state law enforcement agencies to submit data to the Department on any deaths of individuals that occurred during interactions with law enforcement while in their custody. The OIG is reviewing DOJ's actions to implement the Act.

The Department also plays an important role in building trust between police departments and the communities they serve by advocating reforms that increase transparency of law enforcement operations. For example, the COPS Office supports the Police Data Initiative, which promotes the use of "open data." As of July 2017, more than 130 law enforcement and public safety agencies have joined the Police Data Initiative, releasing more than 200 data sets, including accidents and crashes, citizen complaints, calls for service, and officer involved shootings. As of May 2018, more than 50 police agencies have agreed to release data on hate and bias crimes in an effort to increase awareness of the problem. The effort to make more law enforcement data available has the potential to increase public awareness of public safety issues and generate community support for addressing those issues. Yet, more needs to be done to fully realize the initiative's potential as the number of participating agencies accounts for a small fraction of the total law enforcement community in the United States.

Source: Police Data Initiative

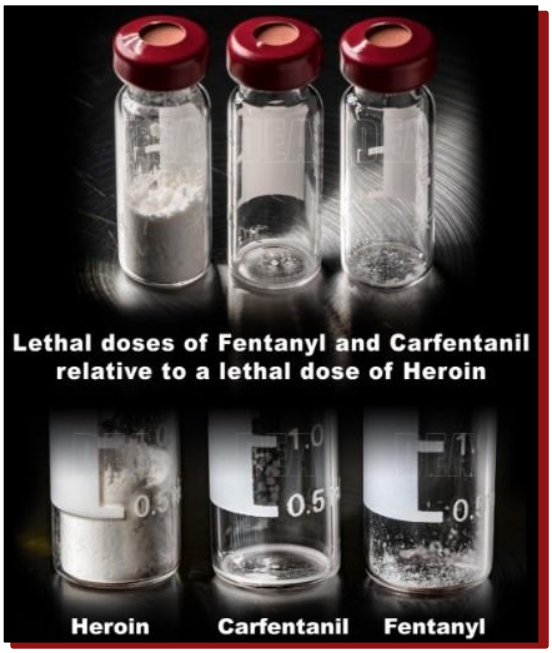
The use of body worn cameras has become more widespread and gained importance in police-community relations in recent years. From FY 2016 - 2018, Congress provided the Department with over $70 million in funding for the Body Worn Camera Partnership Grant Program, which provides matching grants to support the purchase and deployment of this technology to state, local, and tribal public safety agencies. The Department has requested $22.5 million for this program in its FY 2019 budget. A growing body of research suggests that the use of body worn cameras can help build trust between police departments and the communities they serve and reduce use of force incidents and injuries to both officers and civilians. For example, a December 2017 National Institute of Justice (NIJ)-funded study in Las Vegas, Nevada attributed to body worn cameras a 25 percent proportional reduction in officers generating a citizen complaint and a 41 percent proportional reduction in officers generating a use-of-force report. Despite this research, the use of body worn cameras presents issues with regard to officer safety, privacy, criminal discovery, and other legal questions. These issues will challenge the Department in its efforts to support law enforcement agencies on how best to use technology safely and effectively.

COORDINATING WITHIN THE DEPARTMENT AND ACROSS GOVERNMENT TO FULFILL THE DEPARTMENT'S MISSION TO COMBAT CRIME

Combatting crime and promoting public safety is central to the Department's mission, and the effectiveness of DOJ's efforts in this area impacts each of the Department's strategic goals. Addressing the nation's most pressing criminal threats requires effective inter-Department and interagency coordination. While the Department has made important strides in these areas, several challenges remain.

Combatting Drug-Related Crime

The current opioid crisis and its impact on drug-related crime, overdose deaths, and incarcerations continues to present a major challenge for the Department. The Centers for Disease Control and Prevention provisionally estimates that over 72,000 people died in 2017 from drug overdoses. Over 49,000 of those overdose deaths involved opioid analgesics and illicit opioids such as heroin and synthetic opioids. Amplifying this issue is the recent emergence of the synthetic opioid, fentanyl and fentanyl analogs, which accounted for nearly 30,000 estimated overdose deaths in 2017.



Source: DEA

The Department has developed several new initiatives in an effort to address this crisis. For instance, in December 2017, the Department created a new senior level position, the Director of Opioid Enforcement and Prevention, to assist Department leaders and components in formulating and implementing Department initiatives, policies, grants, and programs relating to opioids, and coordinating these efforts with law enforcement. The Department also established the Opioid Fraud and Abuse Detection Unit, a pilot program in 12 U.S. Attorney's Offices (USAO) that utilizes health care fraud data to identify and investigate individuals suspected of diverting controlled substances. Further, in July 2018, given the prevalence of fentanyl overdoses, the Department announced Operation Synthetic Opioid Surge (S.O.S.). The Operation was launched in ten USAOs with some of the highest drug overdose death rates with the goal of prosecuting every readily provable case involving the distribution of fentanyl, fentanyl analogs, and other synthetic opioids, regardless of drug quantity. Given these new enforcement initiatives, it is imperative that the Department establish performance measures to determine the potential impact and effectiveness in combatting the opioid crisis and be able to adapt and refine its various approaches based on these strategic measures.

Source: DEA Fentanyl Response Team

On the regulatory side, in July 2018, the Department announced a rule change that requires the DEA, when establishing its annual opioid production limits, to consider the probability that a drug will be diverted for abuse. This rule change could result in a reduction in the drug amounts that can be lawfully produced in a given year, and therefore limit the amount of opioids available for potential diversion. The OIG has a forthcoming report, which examines the DEA's regulatory enforcement efforts concerning opioids and its coordination with state and local law enforcement partners.

OIG Review: DEA's Opioid Enforcement Efforts

The OIG is conducting a review to examine the DEA's: (1) enforcement policies and procedures to regulate registrants; (2) use of enforcement actions involving distributors of opioids who violate these policies and procedures; and (3) coordination with state and local partners in countering illicit opioid distribution.

The Department also funds numerous programs that partner with local law enforcement and public health agencies to combat drug abuse, misuse, and diversion. Developed in FY 2017, the Comprehensive Opioid Abuse Site-based Program (COAP) is a Bureau of Justice Assistance (BJA) grant program, which provides financial and technical assistance to states, local, and tribal governments to plan and implement comprehensive efforts to identify, treat, and support individuals impacted by the opioid crisis. In addition, the NIJ Drug Courts Program provides an alternative to incarceration for the drug-addicted, including those affected by the opioid crisis. The program addresses addiction through treatment and recovery support services to subsequently reduce recidivism. In its FY 2019 budget request, Office of Justice Programs (OJP), which houses BJA and NIJ, requested a combined $63 million in total funding for the COAP grant and Drug Courts programs. Given the many opioid and drug-related programs and funding opportunities recently developed by the Department, its challenge is to efficiently leverage expertise and coordinate resources with components, as well as state and local law enforcement, to address the nationwide opioid and drug crisis.

Combatting Violent Crime

The Department identified the reduction of violent crime as a goal in its 2018-2022 Strategic Plan. Specifically, the Department's strategic framework for combatting violent crime includes activities intended to: (1) disrupt and dismantle violent transnational crime organizations and gangs, such as Mara Salvatrucha, also known as MS-13; (2) support state, local and tribal partners in making communities safe; (3) protect victims of crime from exploitation and re-victimization; and (4) identify, arrest, and prosecute violent criminals for gun violence and other related violent crimes. To meet these strategic goals, the Department continues to lead or support several violent crime initiatives, including the Organized Crime and Drug Enforcement Task Force's (OCDETF) National Gang Strategic Initiative,

Crime Gun Intelligence Centers (CGIC), and the expansion ATF's National Integrated Ballistic Information Network (NIBIN) Urgent Trace Program.

While combatting violent crime remains a top priority for the Department, an ongoing challenge in meeting this strategic priority is to identify ways to best support state and local law enforcement agencies and prosecutors with limited resources to continue to bring down the level of violent crimes in all jurisdictions. Toward this end, under the PSN initiative, Attorney General Sessions has required all U.S. Attorneys "to engage with a wide variety of stakeholders—from the police chiefs, to sheriffs, to mayors, to community groups and victims' advocates—in order to identify the needs specific to their communities and develop a violent crime reduction plan." The Department reports recent progress in these efforts. For example, according to an October 3, 2018 address by Attorney General Sessions, the murder rate in the 29 largest U.S. cities will decline by 7.6 percent—bringing the murder rate to 2015 levels in those jurisdictions. Additionally, according to a December 2017 NIJ report, BJA's Public Safety Partnership sites "have enhanced relationships and communication with DOJ law enforcement agencies and improved understanding of the range of infrastructure required to develop and maintain the capabilities to effectively combat violent crime." Continued progress in this area will require effective use of the resources Congress has provided for PSN and related initiatives to promote coordination and implementation of crime reduction plans.

OIG Review: Violent Crime Initiatives

The OIG is conducting a review to evaluate the Department's strategic planning and accountability measures for combatting violent crime, including coordination across Department prosecution, law enforcement, and grant making components; and strategic planning for providing assistance to communities that are confronting significant increases in homicides and gun violence.

Ensuring Efficient Coordination to Combat Complex Criminal Threats

The Department faces a number of complex criminal threats – including human trafficking, crimes against children, and crimes in Indian country – which challenge traditional law enforcement approaches. These criminal threats, which often target vulnerable populations, require a dynamic and adaptable response from the Department, as well as effective coordination among the Department's law enforcement components and external partners.

Human trafficking and crimes against children are threats that require increased interagency coordination to enhance the Department's response. The Department participates in several interagency task forces that combat human trafficking. The Department's Civil Rights Division leads the interagency Anti-Trafficking Coordination Team (ACTeam), which combines the efforts of the Department, FBI, DHS, and Department of Labor by working to develop high-impact cases involving labor and sex trafficking. U.S. Attorney's Offices in districts where the program's first phase was launched in 2011 reported an increase of 114 percent in human trafficking cases filed, while defendants convicted in those districts increased by 86 percent. Phase two of the program, which included six additional districts, will be concluding in September 2018. Further, the Department's Internet Crimes Against Children Task Force Program (ICAC) assists state and local law enforcement agencies in developing responses to technology-facilitated child sexual exploitation and other crimes against children. In 2017, the ICAC received over $27 million in funding and task force programs conducted more than 66,000 investigations.

Criminal activity in Indian country is another challenging threat that requires enhanced coordination. The Department's challenge is to coordinate its law enforcement efforts in Indian country to prevent violent crime, while navigating the legal and jurisdictional structure of Indian country and maintaining effective relationships with tribal authorities. Statistics show that Native Americans and others living on tribal lands experience a per capita rate of violent crime twice that of other racial and ethnic groups. This responsibility is heightened by the fact that, in much of Indian country, the Department has the sole

authority to investigate and prosecute when certain felony-level crimes are committed. Recognizing the scope of the challenge facing the Department in Indian country, a 2017 OIG report found a need to increase engagement and coordination, expand law enforcement training necessary for tribal officers, and improve data collection for tribal crimes In April 2017, the Department announced the creation of the Indian Country Federal Law Enforcement Coordination Group, which brings together law enforcement personnel from 12 federal components to increase collaboration and coordination when responding to violent crime in Indian country. The Department also conducted listening sessions with tribal law enforcement in May and June 2017, regarding the most pressing public safety issues in Indian country, including rising violent crime, the opioid crisis, and human trafficking. In August 2018, the Department also announced the expansion of the Tribal Access Data Program, which provides federally recognized Tribes the ability to access and exchange data with the national crime information databases for both civil and criminal purposes to assist in investigations and prosecutions. Although the Department has taken steps to enhance coordination in responding to numerous criminal threats, ensuring and improving efficient agency coordination must remain a top priority in order to promote public safety and ensure that taxpayer funds are spent with the utmost integrity.

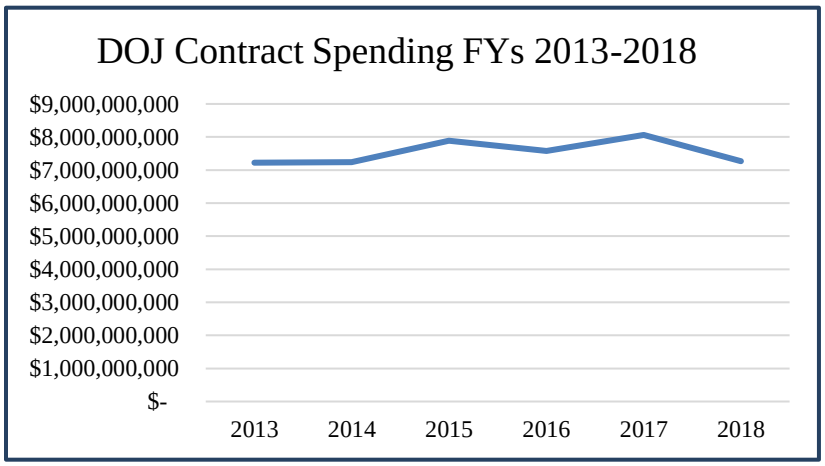
ADMINISTERING AND OVERSEEING CONTRACTS AND GRANTS

The Department expends over $10 billion annually on contracts and grants to fulfill its mission. This represents approximately 36 percent of the Department's $28 billion discretionary budget. Efficient and effective administration and oversight of all DOJ contracts and grants is necessary to ensure that the programs are meeting DOJ and component mission objectives and to protect these tax dollars from waste, fraud, and abuse.

While the Department's contract spending has remained consistent over the past several years, challenges in overseeing and administering contracts persist. During the same period, the Department has increased the amounts awarded through grants, specifically those supported by the Crime Victims Fund (CVF). These funds are critical to accomplishing the Department's goal of protecting and assisting the victims of crime. As a steward of taxpayer funds, it is imperative that the Department provide sufficient administration and oversight of contract and grant funds.

Contracts

Between FY 2013 and FY 2018, the Department's contract spending has remained consistent, averaging about $7.5 billion per year. The OIG will highlight the Department's overall challenges with administering and overseeing contracts in a forthcoming MAM. The MAM will outline areas of concern identified by OIG audits of Department contracts. These include the Department's: (1) inadequate execution of contract oversight responsibilities; (2) insufficient quality assurance practices; and (3) non-compliance with contracting-related laws and regulations. Specifically:



Source: Federal Procurement Data System and USASpending.gov

- In an April 2017 audit of a USMS contract to operate a detention center, the OIG found that the designated Contracting Officer's Representative was tasked with overseeing a contract valued at nearly $700 million with no prior contracting or detention services experience. In a July 2017 audit of an FBI aircraft lease contract, we found that the Contracting Officer did not have the requisite technical expertise to oversee the contract and did not formally appoint a Contracting Officer's Representative to assist in administering and overseeing the contract. Further, in a January 2018 audit of a DEA linguist services contract, we found that the Contracting Officer's Representative was not performing the majority of the responsibilities as identified in the Contracting Officer's Representative designation letter, including the review and approval or disapproval of invoices.
- In a March 2018 audit of a DEA aviation support services contract, valued at $176.6 million, the OIG determined the DEA did not verify labor billing rates or review timesheets, material invoices, and other supporting documentation. The lack of invoice review by the Department has led to several investigations that have resulted in payments back to the Department by contractors

to resolve False Claims Act allegations. In a January 2018 audit of a DEA linguist services contract, the OIG found that the DEA did not develop a quality assurance surveillance plan and performed minimal quality assurance of contract requirements. Additionally, DEA officials did not complete the contractor performance assessment reports for the contract, as required by the Federal Acquisition Regulations (FAR), increasing the risk that other government agencies may unwittingly engage an underperforming or noncompliant contractor instead of a prospective qualified bidder.

- In July 2017, the OIG completed an audit of a FBI aircraft lease contract and found that the contract file did not include market research to support a determination that the price was fair and reasonable. Further, in an April 2018 audit of DEA's Asset Forfeiture Program Task Orders, the OIG found the DEA was decisively involved in the hiring of contract workers, but did not maintain complete contract files to support task order worker selection decisions, including those regarding the hiring of a former DEA agent, who retired amid an OIG investigation into his handling of confidential sources.

  Our recent contract audits have repeatedly found that components provided inadequate guidance and training to personnel responsible for the administration and oversight of complex service contracts. Consequently, we noted that in one instance the Department administered the contract in a manner that created a personal services contract, which makes the contract workers appear to be, in effect, government employees. These contracts are unallowable without statutory authorization, which not all of the Department's components have. Our audits also identified several non-compliances with the Service Contract Labor Standards and potential non-compliances with the Fair Labor Standards Act, which may have affected fair competition and negotiated prices.

In response to OIG audit findings and recommendations, the Department has made some progress towards improving its administration and oversight of its contracts. For instance, the DEA implemented a new requirement that all Task Monitors who oversee its regional linguist contracts must complete FAC-COR Level I training prior to being designated a Task Monitor. The DEA also enhanced its policies regarding interaction between its employees and contract personnel and the adjudication of former DEA employees returning as contract personnel. In addition, the Justice Management Division promulgated a new Acquisition Policy Notice 2018-03, *Service Contract Labor Standards*, which identifies recommended training and resources to which components should refer when awarding and administering service contracts. However, further remedial actions are needed to address lingering systemic issues and to ensure that Department personnel are knowledgeable and equipped to safeguard responsibly the Department's contracts and ultimately taxpayer funds.

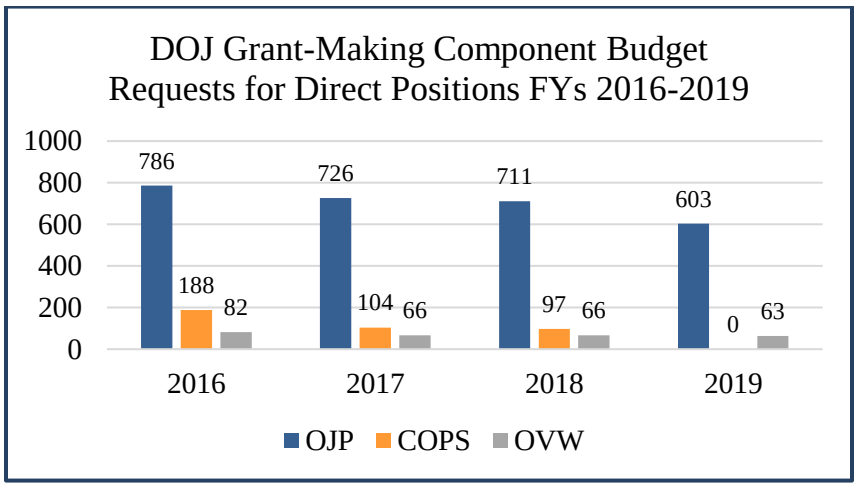
Grants

The Department continues to face challenges in grant management, oversight, and performance monitoring. OIG audits have consistently identified instances of: (1) funding obligated against awards eligible for closeout, (2) unallowable spending undetected by granting agencies, and (3) deficiencies in oversight resulting in overspending.

In prior years' Top Management and Performance Challenges reports, we highlighted the increased responsibility the Department faces in its management of the CVF, due to significant funding increases provided to recipients beginning in FY 2015. The *Victims of Crime Act* established firm deadlines for spending the CVF funding, which creates challenges for both OJP and the state agencies responsible for administering formula awards, especially given that FY 2018 marked the fourth year in a row that CVF funding levels have been significantly higher than historical levels. Also, the FY 2018 CVF funding specifies that 3 percent or about $133 million of the funding shall be available to the Office of Victims of Crime (OVC) for grants to Indian tribes to improve services for victims of crime. This is a significant

increase in funding that presents the Department with additional challenges and will require sufficient oversight and monitoring to ensure proper use of the funds.

The Department's FY 2019 Budget Request included a reduction in staffing at the granting agencies, intended to streamline services, save taxpayer dollars, and eliminate duplication of effort by the granting agencies. The graph below illustrates the number of direct personnel requested, during FYs 2016-2019, by each of the Department's three primary grant-making components: the COPS Office, OJP, and Office on Violence Against Women (OVW).



Source: FY 2019 Budget Requests for the COPS Office, OJP, and OVW

The OIG has previously highlighted the potential overlapping administrative functions between the Department's three grant-making agencies, and efforts to enhance the efficiency of administrative functions in grant-making components are responsive to those concerns. In making these changes, the Department also must ensure that it can effectively manage its grant award processes and monitor grantees to ensure the achievement of grant objectives and accountable stewardship of federal grant funds.

EFFECTIVELY APPLYING PERFORMANCE-BASED MANAGEMENT TO INFORM DECISION MAKING AND IMPROVE OUTCOMES

Effectively incorporating performance management practices into the Department's operations remains a significant challenge that will require a sustained and focused effort. The OIG has included performance-based management in its Top Management and Performance Challenges report every year since 2014, and the importance of addressing this challenge has not diminished over time. If the Department is to succeed in achieving the goals laid out in its newest strategic plan and delivering quality services and timely results to the American public, it will need to consistently collect and analyze performance-related data, employ more outcome-oriented performance metrics, and adopt more innovative approaches in how it uses data to assess performance and inform decision-making.

A Pervasive Challenge for Many Federal Agencies

The Department is not alone in facing the pervasive and long-standing challenge of effectively implementing performance-based management. In April 2018, the Council of the Inspectors General on Integrity and Efficiency (CIGIE) released its first-ever report of the top management and performance challenges facing multiple federal agencies. Performance-based management was among the seven challenges most frequently cited in management and challenges reports created by individual federal OIGs in 2017, and we at the DOJ OIG have highlighted in prior reviews numerous programs where this concern is applicable to the Department. For example, the OIG found ineffective performance measures in recent reviews of BOP's healthcare and rehabilitation services, DEA's and ATF's confidential informant programs, and DOJ efforts to combat violent crime. Separately, the GAO has completed over 30 reviews related to federal agency implementation of the *Government Performance and Results Act (GPRA) Modernization Act of 2010* (GPRAMA) and corresponding guidance from the Office of Management and Budget's (OMB) Circular A-11, which establishes the framework that federal agencies are required to follow to enhance their performance and management and provide greater accountability for results. These reports identify numerous challenges that agencies have faced in implementing GPRAMA's performance management requirements. Additionally, 2017 GAO survey data showed that federal managers' reported use of performance information in decision-making generally had not improved and in some cases was lower than it was 20 years ago.

The Department's FY 2018-2022 Strategic Plan presents an opportunity for the Department to embrace more fully not only the requirements of the *GPRAMA*, but also the spirit of the law. The Strategic Plan includes four strategic goals, three agency priority goals, 11 strategic objectives, and 37 performance measures. The three agency priority goals, which serve as the Department's priorities for the first two years of the plan and are subject to quarterly data-driven performance reviews, include (1) combatting cyber-based threats and attacks, (2) combatting violent crime, and (3) disrupting and dismantling drug trafficking organizations to curb opioid and other illicit drug use. In September 2018, the Department began reporting through Performance.gov its progress in meeting the agency priority goals with performance data. However, the Department has not yet prepared its annual performance plan for FY 2019, and consequently has not identified or communicated the performance measure targets in the strategic plan that it plans to achieve in FY 2019 and the strategies it will follow to do so. In addition, four of the Department's annual performance measures related to its strategic objective to reduce violent crime are still under development. The Department's three agency priority goals address themes we have identified as challenges in this year's Top Management and Performance Challenges report, and we discuss each in more detail in the sections on Cybersecurity, Combatting Crime, and Building Trust between Law Enforcement and Communities.

In prior years' Top Management and Performance Challenges reports, we noted that the nature of much of the Department's work does not lend itself to programmatic outcomes that can be easily measured. However, the Department must continue to explore ways it can develop meaningful performance metrics that are data-driven, outcome-oriented, and not based solely on measurements of processes or outputs. The OIG will continue to monitor the Department's performance management activities as it strives to achieve the goals contained in its strategic plan.

OIG Review: Performance Management of the Department's Violent Crime Programs and Initiatives

The OIG is conducting a review to evaluate the Department's strategic planning and accountability measures in combatting violent crime, including coordination across the Department's prosecution, law enforcement, and grant making components, and strategic planning for providing assistance to communities that are confronting significant increases in homicides and gun violence.

Measuring the Effectiveness of Department Programs with Accurate Data and Relevant Metrics

Recent policy developments hold promise for the Department's adoption of data-driven practices and evidence-based management, or the use of empirical knowledge and research-supported principles to inform decision-making. In 2018, OMB released the President's Management Agenda, which calls for the smarter use of data and evidence-based approaches to guide decision making. In addition, the *Commission on Evidence-Based Policymaking Act of 2016* mandated the Commission to develop a strategy for how data the government already collects can be used to improve government programs and policies while protecting privacy and confidentiality. The Commission's final report, issued in September 2017, included several recommendations for fundamental improvements to the federal government's evidence-building systems and capabilities. The report also identified existing government data that has the potential to be useful for evidence building, such as the FBI's National Incident-Based Reporting System (NIBRS), which provides detailed crime incident data, and statistical data on criminal justice systems collected by the Bureau of Justice Statistics.

Performance data is crucial to evaluating the Department and its components' effectiveness in meeting their policy goals, as well as ensuring that future strategies and initiatives are both appropriate and evidence-based. With accurate and valid performance data, the Department can make improvements to its programs and also highlight areas of success. However, OIG work has shown that the Department's ability to obtain and use the right data to measure program performance remains an ongoing challenge. For example, a 2017 OIG report found that BOP cannot accurately determine the number of inmates who have mental illness because institution staff do not always document mental disorders, which leaves BOP unable to ensure that it is providing them with appropriate care. Similarly, an OIG review of the BOP's reimbursement rates for outside medical care found that the BOP's failure to use all-electronic medical claims greatly limited its ability to obtain and analyze data that could help it to achieve greater efficiencies and reduce the cost of medical care. Furthermore, a 2017 OIG report found that crime data in Indian country remains unreliable and incomplete, limiting the Department's ability to comply with its law enforcement responsibilities pursuant to the *Tribal Law and Order Act of 2010*. In yet another example, the OIG recommended in a 2017 report that the Department collect relevant and timely charging data to more accurately assess the implementation and impact of its charging policies and practices.

The Department has also struggled to use outcome-oriented measures to monitor whether its programs are accomplishing their intended goals. For example, a 2018 GAO report found that only one of the five federal strategies to combat synthetic opioids that it examined included outcome-based performance

measures. Among the strategies that included only output-focused measures was the Department's 360 Strategy, which uses metrics such as the number of participants in its opioid demand reduction activities. Measures like this fail to convey the significance and impact of the Department's efforts, and therefore must be accompanied or replaced by those that meaningfully link inputs to outcomes. A 2017 OIG audit of the risks associated with the management of the Crime Victims Fund Grant Programs also found that the programs' goal and objectives are neither outcome-oriented nor expressed in a quantitative and measureable form. In contrast, a 2018 OIG audit found that the Civil Rights Division began incorporating outcome measures in its consent decrees for police misconduct cases to demonstrate that the process improvement actually resulted in greater constitutional policing or increased confidence by local communities in their policing authorities.

The Department must continue its efforts to collect and use meaningful performance data and use relevant metrics to improve program performance. The improved use of data and outcome-based metrics will help the Department better grasp the challenges associated with its programs so that it may address issues that arise, as well as evaluate progress toward its intended goals.

Identifying Areas of Risk Using Data Analytics

In addition to measuring the effectiveness of the Department's programs, performance-based management can proactively identify areas of risk within the Department. Performance-based data, if correctly collected and analyzed, can point to areas of fraud, waste, and abuse within Department programs. The OIG created our Office of Data Analytics (ODA) to use statistical analysis, mathematical modeling, and data visualization to detect and deter fraud, waste, and abuse and misconduct in Department programs and personnel. In a December 2017 report, ODA efforts and investigative activity revealed that BOP has incomplete and inadequate healthcare claims data in electronic format and that the claims adjudication vendor has not provided all contractually required services, including fraud monitoring. The OIG found that, as of February 2017, only 16 of BOP's 122 institutions were submitting electronic claims for processing by the claims adjudication vendor, while the remaining 106 BOP institutions were processing claims from BOP's health care contracts manually in a paper-driven process. Incomplete claims data and ineffective analysis of that data significantly increases the BOP's fraud risks and diminishes both the BOP's and the OIG's ability to detect past and present fraud schemes. The OIG recommended that BOP move to immediately require all contractors to submit electronic claims, ensure those claims are properly analyzed and maintained by BOP's adjudication vendor, and enforce existing contract language that requires the adjudication vendor to perform fraud analytics and report any indicators of fraud to the BOP.

As the Department continues to implement the concepts of performance-based management, it should explore additional techniques to leverage data analytics to assist in meeting this challenge. For example, as mentioned in the *Cybersecurity* section of this report, the Department has indicated that it is taking steps to enhance its insider threat detection efforts through continuous monitoring and proactive analysis of user activities on Department IT systems for suspicious activity. The use of data analytics can also assist the Department in finding program deficiencies and identifying needed improvements.

FILLING MISSION CRITICAL POSITIONS DESPITE DEPARTMENT CHALLENGES AND DELAYS IN THE ONBOARDING PROCESS

To meet 21st century demands, the Department must develop innovative solutions to address challenges relating to the recruitment and retention of a professional, highly competent, and diverse workforce. These challenges include recruiting professionals in the cybersecurity and healthcare fields and in the timely processing of background checks to prevent undue delay in the onboarding of new personnel. The Department must also take steps to ensure that its hiring and promotion policies and practices are equitable, particularly in law enforcement positions.

Recruiting and Retaining Skilled Experts in the High Demand Cybersecurity and Healthcare Fields

As noted in last year's report, the recruitment and retention of professionals in the cybersecurity and healthcare fields remains a challenge for the Department. The restrictions of the federal pay scale and stringent background requirements pose significant hurdles for the Department in the struggle to compete with the private sector and other federal entities with special hiring authorities for personnel with these high-demand, specialized skills. The frequency and impact of cyber-attacks on our nation's private sector and government networks and infrastructure have increased dramatically in the past decade. As noted in this report's chapter on cybersecurity, the Department must recruit and retain a cyber-workforce that is capable of responding to cyber-attacks internal and external to the U.S. government.

Cyber professionals are in high-demand in the private sector, often putting the federal government at a competitive disadvantage in the recruitment of individuals with specialized IT skills. In response to this challenge, on February 16, 2018, Attorney General Sessions directed the formation of a Cyber-Digital Task Force to assess the Department's work in the cyber arena, and to identify how federal law enforcement can more effectively accomplish its mission in this vital and evolving area. This task force produced a report on July 2, 2018 that, among other things, recommended: (1) the recruitment and retention of attorneys, investigators, and professional staff with the necessary skills to combat cyber threats and (2) the strengthening of the Department's tools and legislative authorities to advance current cyber initiatives.

An ongoing impediment to the recruitment of candidates with these high-demand technical skills is the Department's difficulty in offering salaries that are competitive with the private sector. In April 2017, GAO's Director of Cybersecurity and Information Management Issues testified that salary restrictions impede the federal government's ability to retain talented employees. Moreover, in March 2018, the FBI Director remarked that the bureau is trying to maximize its use of private sector partners to combat cyber threats, but a major challenge is the recruitment, hiring, and training of IT professionals, within and outside of the FBI.

The Department also continues to face significant challenges recruiting and retaining medical professionals largely due to competition from the private sector, which offers higher pay and benefits. As noted in last year's Top Management and Performance Challenges report, the salaries and incentives needed to compensate BOP employees for the safety, security, and remote location factors unique to workers in a correctional facility, pose challenges to the recruitment of medical personnel to the BOP. In April 2018, the OIG found that while BOP has begun to develop a plan to use available data to assess and prioritize medical vacancies, the percentage of authorized medical positions that were vacant between 2016 and 2017 increased from 15 percent to 21 percent. Additionally, during that same one-year period,

only 17 percent of BOP requested medical staff positions were filled. Moreover, despite a January 2018 request by BOP to use available incentives to fill psychiatrist positions, the BOP remains unable to fill many staff psychologist positions at restrictive housing institutions. The Department's ability to attract and retain highly-skilled individuals is critical to helping the Department achieve its mission.

Building a Diverse Workforce by Ensuring Equitable Hiring Policies and Practices

The Department must also ensure that its workforce reflects the diversity of the U.S. civilian labor force by promoting equitable policies. The Department's FY 2018-2022 Strategic Plan sets a goal to develop its workforce by enhancing the skill set of current employees and hiring "diverse, dedicated individuals to meet the Department's needs."

FY 2016 DOJ Law Enforcement Component Workforce					
	ATF	DEA	FBI	USMS	All Four Components
Total Workforce	5,195	8,936	37,029	5,229	56,389
Number of Female Staff	1,670	3,172	16,038	1,269	22,149
Percentage of Female Staff	32.1	35.5	43.3	24.3	39.3

Source: FY 2016 DOJ Employment Fact Book

As the OIG noted in a June 2018 report, a "Review of Gender Equity in the Department's Law Enforcement Components," while the ATF, DEA, FBI, and USMS have taken steps to increase diversity, additional resources should be deployed to address concerns related to gender equity for the promotion of an equitable culture. To illustrate, the OIG found that women accounted for only 16 percent of Criminal Investigators in DOJ's law enforcement components. Additionally, women held few headquarters executive leadership positions over operational units and few top field leadership positions. Among Criminal Investigators, women did not receive a proportionate amount of promotions based on the potential applicant pool. Many female Criminal Investigators at ATF, DEA, and FBI believed there was a "glass ceiling" for women. We made six recommendations to address these issues, all of which remain pending.

Other Obstacles to Filling Critical National Security, Immigration, and Leadership Positions Within DOJ

As the rate of federal retirements continues to increase, it is imperative that the Department identifies and hires the most qualified personnel to replace that lost talent as quickly as possible. As part of the hiring process, Department employees must undergo background investigations designed to ensure that they are reliable, trustworthy, of good conduct and character, and of complete and unwavering loyalty to the United States. Delays in completing background investigations for prospective employees can have a material impact on the Department's operations. Further, many of the Department's mission critical positions also require National Security Information clearances, which can add time to the onboarding process. In September 2017, GAO reported that the executive branch has been unable to process security clearances in a timely manner, causing a significant backlog of background investigations, totaling more than 700,000 cases. The slow pace of background investigations hinders the Department's ability to compete with other markets and attract the most qualified candidates for critical Department operations. To meet this challenge, the Department must coordinate with the Office of Personnel Management (OPM) to seek efficiencies in the background check and reinvestigation process and improve on-boarding time, particularly for positions deemed mission critical.

The Department has moved to address a backlog of over 650,000 pending immigration cases by hiring

additional immigration judges using a more streamlined approach to hiring. The new plan emphasizes using clear deadlines to ensure that immigration judge candidates move efficiently through the hiring process. As a result, the Department has reduced hiring times for immigration judges by more than 50 percent since 2010. Specifically, the Executive Office for Immigration Review reported that hiring times have decreased from 742 days to 266 days. In an area which the Department identified a significant need, the Department has identified ways to improve the hiring process, and should consider adapting these approaches to other mission critical areas.

The Department's challenges related to filling critical positions are not uncommon to federal agencies and solutions to overcoming the obstacles of federal hiring are not entirely contingent upon improvements within the Department. The Department must continue to seek out opportunities to streamline internal processes and to coordinate with OPM. While OPM has contracted with the National Background Investigations Bureau to help reduce the backlog of investigations, additional work is required to address this government-wide problem. In the meantime, the Department has utilized a waiver process to help expedite the onboarding of new employees and an interim security clearance approval process to help expedite access to national security information in support of the DOJ mission. However, these are not long-term solutions to this longstanding challenge.

ENSURING ADHERENCE TO ESTABLISHED DEPARTMENT POLICIES AND PROCEDURES

The Department and its components have established policies and procedures to promote and ensure accountability, consistency, and objectivity in DOJ operations. These policies and procedures govern DOJ, both in its role as a law enforcement entity and an employer. Recent OIG work has identified instances in which established policies and procedures were not consistently adhered to, including in some cases by senior Department officials. As noted in recent OIG reports, it is through adherence to its established principles and norms that the Department earns the confidence of the public and its employees.

The OIG's June 2018 *Review of Various Actions by the Federal Bureau of Investigation and Department of Justice in Advance of the 2016 Election* (pre-election report) focused on the actions taken by the FBI and Department during the course of the Clinton email investigation. The OIG made numerous findings in the pre-election report that involved violations of established policies. For example, we found that then FBI Director James Comey chose to deviate from the FBI's and the Department's established procedures and norms and engaged in his own subjective, ad hoc decision making when he decided to make a public announcement in July 2016 about his conclusion that prosecution was not warranted. In doing so, he also made statements about former Secretary Hillary Clinton's uncharged conduct. Moreover, in October and November 2016, shortly before the presidential election, former Director Comey notified Congress of investigative developments in the case and steps the FBI was taking. The July announcement was inconsistent with his role as the FBI director, and violated long-standing Department policy, practice, and protocol. Similarly, Comey's subsequent notifications to Congress about the renewed investigation violated the established policy of not commenting on pending investigations.

In addition, the OIG found that the FBI's media policy, which strictly limits the employees who are authorized to speak to the media, appeared to be widely ignored during the pre-election period that we reviewed. We identified numerous FBI employees, at all levels of the organization and with no official reason to be in contact with the media, who were nevertheless in frequent contact with reporters. We found that the harm caused by leaks, fear of potential leaks, and a culture of unauthorized media contacts influenced FBI officials on consequential investigative decisions. The FBI has strengthened its media contact policy, but faces the continuing challenge of enforcing it to address the harmful culture of unauthorized disclosures of sensitive investigative information.

The pre-election report also found that several FBI employees who played critical roles in the investigation used FBI devices to send political messages—some of which related directly to the investigation. These messages created the appearance of bias and thereby raised questions about the objectivity and thoroughness of the investigation. As noted in the report, using FBI devices to send such messages—particularly the messages that intermix work-related discussions with political commentary—potentially implicate provisions in the FBI's Offense Code and Penalty Guidelines. The report also identified instances in which senior FBI officials who had leadership and supervisory responsibilities over the investigation into Secretary Clinton's use of private email used their own private email accounts for official government business. The report found that such use of a personal email account for unclassified FBI business to be inconsistent with Department policy.

A lack of consistent adherence to established Department policies is not limited to the issues we identified in the pre-election review. For example, recent OIG audits of the DEA's and ATF's confidential source programs identified systemic concerns with DEA's and ATF's use and payment of confidential sources. These failures create significant risks for the Department, in cases where mishandled informants

prejudiced prosecutions and other Department operations. In a March 2017 report, the OIG found, among other things, that ATF did not adequately maintain payment information for all of its CIs and ATF could not readily provide accurate, complete, and reliable information from its National CI Registry System about certain types of CIs for whom there is an elevated element of risk involved in their use or management. Similarly, in a September 2016 report, the OIG found, among other things, that the DEA did not appropriately track all confidential source activity and had violated its own policies by paying millions of dollars to confidential informants who previously had been "deactivated" because of an arrest warrant or for committing a serious offense. The OIG is currently auditing the FBI's Confidential Human Source Program.

The Department faces similar challenges as an employer. Department-wide adherence to personnel laws, policies, and practices applicable to all federal employees is necessary to promote a productive, merit-based work environment and to ensure that employees are not fearful of retaliation or harassment. The OIG's work in the recent past has demonstrated that the Department faces an ongoing challenge of providing a workplace free from harassment and intimidation.

First, whistleblowers perform an important function. Government employees have unique insight into the problems that exist within agencies. In recognition of the critical need for whistleblowers to come forward, Congress passed the Whistleblower Protection Act (WPA) in 1989, which protects employees who make lawful disclosures of misconduct and provides a remedy for any reprisal resulting from their protected disclosures. In 2017, in legislation to re-authorize the U.S. Office of Special Counsel, Congress created mandatory requirements for agencies to inform their employees about these protections and to ensure that all federal supervisors are aware of their responsibilities under the WPA.

The Department continues to face challenges with its employees respecting the role of whistleblowers. Over the past two years, the OIG has found 5 instances of retaliation against whistleblowers. In each instance, the managers failed to recognize and adhere to clear laws and policies that protect employees for disclosing evidence of misconduct to lawful recipients. In the past year, the OIG has twice provided recommendations to Department components to enhance its education of managers about whistleblower protections and to ensure that their policies and the policies of Department contractors comply with the legal requirements.

Department leadership is aware of this concern and is responsive to the OIG's efforts to enhance education of DOJ employees about whistleblower rights and protections. For example, Deputy Attorney General Rosenstein contributed to a recent OIG training video and discussed the importance of whistleblowers. Similarly, FBI leadership has been proactive in seeking to train its managers on the important role of whistleblowers and the protections they are entitled to under the law. The Inspector General has been invited to speak to the issue at annual conferences for Field Office Special Agents in Charge and other meetings of FBI senior leaders.

Second, as evidenced by the OIG's June 2017 report on the Civil Division's handling of sexual harassment and misconduct allegations, the Department faces a continuing challenge of maintaining a workplace free of sexual harassment. Notwithstanding the Department's "zero tolerance policy" with regard to sexual harassment, the OIG found significant inconsistencies among penalties imposed by the Civil Division for substantiated harassment allegations, as well as weaknesses in its tracking of allegations. The OIG's findings in the Civil Division do not appear to be isolated. Over the past two years, OIG investigations have substantiated sexual harassment or related allegations in numerous cases in 7 other Department components. In one recent case, the OIG found that a supervisory attorney in a Department division sexually harassed a subordinate by making unwanted sexual advances, and that a second supervisory attorney instructed a subordinate not to discuss the harassment in violation of laws that protect employees for reporting such misconduct. In another case, the OIG concluded that a senior

Department official sexually harassed several subordinates, and sexually assaulted one, over a period of at least 10 years. In response to the OIG's Civil Division report, the Deputy Attorney General formed a working group, and the Department issued new guidance to all Department components in April 2018 to enhance awareness of and ensure appropriate response to substantiated allegations of sexual harassment in the DOJ workplace.

As we concluded in the pre-election report, by adhering to its established procedures, principles, and norms, the Department better protects the interests of both federal law enforcement and its own dedicated professionals, as well as providing the public with greater confidence in the outcome of its decisions. This is a challenge that the Department must continue to strive to address.