OIG Top Management and Performance Challenges Facing the Department of Justice – 2017

October 16, 2017

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 2017 list of top management and performance challenges facing the Department of Justice (Department), which we have identified based on our oversight work, research, and judgment. We have prepared similar lists since 1998. By statute, this list is required to be included in the Department's Agency Financial Report.

This year's list identifies eight challenges that we believe represent the most pressing concerns for the Department:

- *Safeguarding National Security and Ensuring Privacy and Civil Liberties Protections*
- *Enhancing Cybersecurity in an Era of Increasing Threats*
- *Managing an Overcrowded Federal Prison System in an Era of Declining Resources*
- *Strengthening the Relationships Between Law Enforcement and Local Communities and Promoting Public Trust*
- *Coordinating within the Department and Across Government to Fulfill the Department's Mission to Combat Crime*
- *Administering and Overseeing Contracts and Grants*
- *Using Performance-Based Management To Improve Department Programs*
- *Filling Mission Critical Positions Despite Competition for Highly-Skilled Professionals and Delays in the Onboarding Process*

We believe that safeguarding national security and enhancing cybersecurity in the face of evolving threats are particular challenges that will be at the forefront of the Department's attention and require vigilance for the foreseeable future. In addition, this year's list again includes the challenge *Using Performance-Based Management to Improve Department Programs,* which we believe continues to grow in importance. Moreover, this challenge impacts many of the challenges listed above, illustrating how the deficit in performance-based management can hinder the Department's ability to accomplish its mission efficiently and effectively. Meeting all of these challenges will require the Department to develop innovative solutions and exercise careful oversight to ensure the effectiveness of its operations.

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

Attachment.

This page intentionally left blank.

TOP MANAGEMENT AND PERFORMANCE CHALLENGES FACING THE DEPARTMENT OF JUSTICE

Office of the Inspector General

Safeguarding National Security and Ensuring Privacy and Civil Liberties Protections

National security has been the U.S. Department of Justice's (Department) highest priority since the attacks of September 11, 2001, and this prioritization remains unchanged in Fiscal Year (FY) 2018. Protecting the United States from terrorism, both foreign and domestic, and promoting national security consistent with the rule of law is the Department's primary strategic goal. The Department also contributes to protecting the nation from increasingly complex foreign intelligence threats. Adversaries' motivations and tactics constantly evolve, as do the technologies they rely upon. Keeping pace in this dynamic environment poses a significant challenge and is a key concern of the Department, which must leverage effective technologies and legal authorities, and apply them in a manner that protects the privacy and civil liberties of the public.

Combating Foreign and Domestic Terrorism

The Federal Bureau of Investigation (FBI) leads the Department's counterterrorism efforts and, in FY 2016, dedicated over 7,000 full time employees and more than $2 billion to this key mission area. One counterterrorism challenge is the threat posed by Homegrown Violent Extremists (HVE), defined as individuals who reside or operate in the United States and are inspired to act on behalf of a foreign terrorist organization, such as al Qaeda or the Islamic State of Iraq and al-Sham (ISIS). FBI HVE investigations span all 50 states and the Director of the National Counterterrorism Center recently stated that "HVEs present the most immediate and unpredictable threat in the United States." The Office of the Inspector General (OIG) is conducting an audit of the FBI's efforts to address HVEs that will evaluate the FBI's policies and procedures used to identify and investigate these threats.

The FBI continues to identify individuals who seek to join the ranks of foreign fighters traveling in support of ISIS. As of March 2017, the FBI estimated that 300 Americans traveled or attempted to travel to Syria to participate in the conflict. The threat posed by ISIS continues to evolve and creates new challenges for the Department as ISIS reacts to a sustained loss of territory. According to a July 2017 report by the Government Accountability Office (GAO), as ISIS loses territory, the group may increase its efforts to encourage followers to conduct attacks in their home countries in order to sustain ISIS's visibility.

Source: FBI

The Department's National Security Division (NSD) also plays a critical role in the Department's counterterrorism efforts and is responsible for overseeing terrorism investigations and prosecutions. According to the NSD, between March 2013 and March 2017, it publicly charged more than 120 individuals either for being a foreign terrorist fighter or for engaging in HVE-related conduct.

The Department's counterterrorism mission is interconnected with those of its federal, state, and local law enforcement partners. Therefore, the United States' national security depends on the ability to share the right information with the right people at the right time. In March 2017, Inspectors General (IG) from the Department of Justice, Department of Homeland Security (DHS), and Intelligence Community issued a joint report on the domestic sharing of counterterrorism information. The IGs concluded that these entities could enhance coordination and collaboration by updating or establishing new information sharing agreements. We also determined that the Department can improve its internal counterterrorism information sharing efforts by implementing a consolidated strategy that aligns with the President's strategic plan and ensures that Department components understand their respective roles and responsibilities.

While attacks directed or inspired by foreign terrorist organizations are deservedly the focus of extensive media coverage, the threat posed by domestic terrorists and domestic extremist ideologies remains serious. According to GAO, between September 12, 2001, and the end of 2016, far-right violent extremists killed 106 people in 62 incidents; during the same time frame, 119 people were killed by radical Islamist violent extremists in 23 incidents. As an example, the Attorney General stated that the August 2017 fatal car attack in Charlottesville, Virginia, meets the federal legal definition of domestic terrorism.

In 2011, the federal government developed a national strategy for countering violent extremism (CVE) that aimed to address the root causes of violent extremism through community engagement. The Department shares responsibility with DHS in efforts to counter violent extremism and co-leads the CVE Task Force. However, GAO's April 2017 report determined that the CVE Task Force had not established a process for assessing whether the federal government's CVE efforts were working.

OIG Report: The WITSEC Program

Another valuable counterterrorism tool is the federal Witness Security Program (WITSEC Program), which provides for the security, health, and safety of government witnesses whose lives are at risk as a result of their testimony against major criminals. In September 2017, the OIG issued a follow-up report on the Department's handling of known or suspected terrorists (KST) admitted into the WITSEC Program. We determined that while the Department has created policies and procedures to address known risks posed by KSTs admitted into the WITSEC Program, it has not sufficiently and appropriately implemented all of them. The OIG remains concerned that the Department has not ensured that KST information has been shared appropriately and in a timely fashion with relevant national security stakeholders, and that those responsible for monitoring KSTs have the information necessary to do so effectively.

Identifying and bringing those who commit terrorist acts to justice is a priority for the Department; however, incarcerating these individuals does not necessarily eliminate the threat. The Federal Bureau of Prisons (BOP) houses inmates who have a history of or nexus to terrorism and is responsible for ensuring that federal prisons are not being used to recruit terrorists or spread extremist ideologies. The OIG is conducting an audit of the BOP's counterterrorism efforts that includes an examination of the BOP's policies, procedures, and practices for monitoring inmates with known or suspected ties to domestic and foreign terrorism. The audit will also consider the BOP's efforts to prevent the radicalization of those with no known terrorism ties upon entry into the BOP system.

Counterintelligence and Counterespionage

Foreign intelligence entities continue their espionage and intelligence-gathering operations against our nation's public and private sectors, seeking access to information such as sensitive military plans, political strategies, intellectual property, economic information, and personally identifiable information. The FBI noted that today's counterintelligence threat "encompasses far more than traditional hostile intelligence service activities," and includes a full spectrum of counterintelligence activities such as economic espionage,

foreign investment, and disruption of supply chains. Defeating our adversaries' intelligence and espionage efforts remains a top priority for the Department.

According to a 2017 joint statement to the Senate Armed Services Committee by senior U.S. intelligence leadership, "the most significant counterintelligence threat . . . involves the rapid development and proliferation of disruptive, advanced technologies that provide adversaries with capabilities that even just a few years ago were not considered plausible." Similarly, the NSD noted in its FY 2018 budget request that "the rapid expansion and evolution of cyber threats" is one of its most significant national security challenges. For a detailed discussion of the cyber challenge to national security, see the *Cybersecurity* section of this report.

OIG Report: The *Foreign Agents Registration Act*

The *Foreign Agents Registration Act of 1938* (FARA), 22 U.S.C § 611 et seq., is a disclosure statute that requires persons acting as agents of foreign principals in a political or quasi-political capacity to make periodic public disclosure of their relationship with the foreign principal.

The Act serves as a valuable counterintelligence and counterespionage tool to help identify and track individuals acting as agents of foreign principals within the United States. In its September 2016 report on the NSD's administration and enforcement of FARA, the OIG found, among other issues, that NSD attorneys and FBI agents interpreted the statute differently and that criminal enforcement of FARA between 1966 and 2015 was minimal, with only seven criminal cases filed during that time frame.

Trusted insiders also pose a serious threat to national security. An insider threat is defined by the government's National Insider Threat Task Force as a threat posed to U.S. national security by someone who misuses or betrays, wittingly or unwittingly, their authorized access to any U.S. Government resource. This can include damage through espionage, terrorism, unauthorized disclosure of national security information, or the loss or degradation of departmental resources or capabilities. Past high profile insider threats include large amounts of highly classified national security information disclosed by Army Intelligence Analyst Chelsea Manning in 2010, and by National Security Agency contractor Edward Snowden in 2013. More recently, in 2016, FBI employee Kun Shan Chun was convicted of illegally acting as an agent of a foreign government after exploiting his inside access at the FBI to provide sensitive information to the Chinese government. Likewise, an employee for a defense contractor in California was sentenced for selling sensitive military and commercial satellite information he stole from his employer to an undercover FBI agent posing as a Russian agent. A September 2017 OIG report on the FBI's Insider Threat Program highlighted several areas that the FBI can improve to better deter, detect, and mitigate insider threats, including ensuring that the FBI notifies the OIG of all insider threat investigations.

Leveraging National Security Legal Authorities While Safeguarding Civil Liberties

The Department faces challenges in leveraging the use of existing legal authorities to identify, locate, and prosecute criminals threatening our national security, while safeguarding the civil liberties of U.S. citizens and residents.

A key piece of legislation used to identify potential terrorists and foreign actors is Section 702 of the *Foreign Intelligence Surveillance Act* (FISA) *Amendments Act,* which expires on December 31, 2017, unless reauthorized by Congress. Section 702 permits the government to compel the assistance of electronic communication service providers to target foreign persons reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. The Attorney General has stated that reauthorization of the FISA Amendments Act is the top legislative priority of the Department and the Intelligence Community because the Act allows the Intelligence Community to collect vital information on individuals and entities threatening national security, such as international terrorists and overseas foreign intelligence targets. Privacy advocates have raised concerns about the FBI's ability to use U.S. person

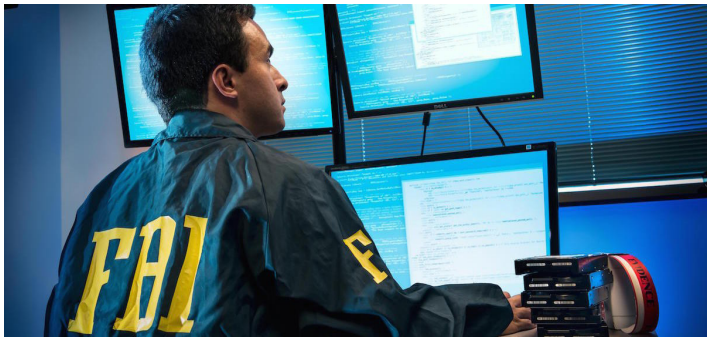
identifiers to query repositories of Section 702 data without a warrant for evidence of crimes that do not relate to national security, as well as concerns that the government is not consistently notifying defendants when Section 702-derived information is used as evidence in criminal proceedings, as required by statute. The Department faces challenges in assuring Congress and the American public that the safeguards built into Section 702, including robust oversight by the NSD and relevant Offices of Inspectors General, minimize the collection, retention, and dissemination of information on U.S. persons while effectively targeting foreign operatives overseas.

The Department's involvement in ongoing legal proceedings with technology companies highlights the challenges that rapidly evolving technologies present to the Department's effort to safeguard national security. For example, the Department has identified the use of social media as a critical tool that terror groups use for radicalization, recruitment, and the development of extremist networks, and continues to engage the private sector in combatting the online efforts of terrorist organizations. However, combatting the threat to the nation's security posed by social media poses unique challenges to the Department. The Department is currently engaged in ongoing litigation with Twitter regarding the public disclosure of the volume of national security letters the company received from the Department. The Department also faces certain legal challenges concerning digital material. For instance, in October 2017, the Supreme Court granted the Department's petition asking the Court to review a lower court's decision that Microsoft is not required to hand over customer data relevant to federal investigations in response to a search warrant if that data is stored on computers located outside the United States. Technology companies, such as Twitter and Microsoft, have been encouraging Congress to revise online privacy laws in recent years, advocating for increased judicial oversight for government queries of Section 702-derived information and a more narrow definition of what constitutes "foreign intelligence information." These examples illustrate the challenges faced by the Department as a result of the growing tension between the government's efforts to safeguard national security and technology companies' efforts to protect customer privacy and respond to user concerns about the nature and extent of government surveillance.

Enhancing Cybersecurity in an Era of Increasing Threats

Defending Against Cyber Intrusions and Attacks

Protecting the nation against cyber-based attacks and high-technology crimes is one of the Department's top priorities. Cyber intrusions and attacks can undermine U.S. military advantage and result in national security breaches, economic losses, failures in critical infrastructure, and intellectual property theft. Cyber intrusions and attacks are occurring more frequently and are becoming more sophisticated and dangerous. There have been a significant number of cyber intrusions of public and private sector systems, including Russia's cyber operations during the 2016 U.S. elections and the compromise of millions of Americans' personal information at the Equifax credit bureau.



Source: FBI

According to the National Institute of Standards and Technology, there have been over 95,330 known cybersecurity vulnerabilities and exposures identified as of September 2017. The growing threats posed by cyber intrusions and attacks affect the government and private sector alike. The OIG is currently evaluating the effectiveness of the FBI's process for notifying and engaging with victims of cyber intrusions. Engagement with private sector victims of cyber intrusions is important both to protect vital infrastructure and as a source of information and intelligence to help the FBI counter 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.

Cybercrime Challenges

In today's digital age, the pervasiveness and global nature of the internet allows criminal groups increased access through our borders and into our lives. The Department anticipates that the growth of sophisticated, global cyber threats will cause damage estimated at over $2 trillion worldwide by 2019. In December 2016, the Assistant Attorney General for the Criminal Division described significant cybercrime challenges, including "loopholes in legal authorities," "the widespread use of warrant-proof encryption," and "inefficient cross-border access to electronic evidence."

The Department has identified gaps in legal authorities that cause 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 proper access to a system who exceeds their authority on that system by improperly disclosing sensitive information may not be subject to criminal prosecution. 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. Botnets, a network of computers created by malware and controlled remotely without the knowledge of the computer's user, also present legal challenges

as the botnets evolve and increase in sophistication faster than the law's ability to adapt to address the threat. Additionally, cybercriminals are increasingly selling or renting access to botnets, actions that are not explicitly criminalized under the CFAA. Although the Department has successfully prosecuted botnet cases pursuant to the CFAA, such as the August 2017 conviction of a Russian citizen for his involvement in a global botnet conspiracy, the CFAA loopholes continue to create a challenge for the Department's cyber investigators and prosecutors.

Striking the proper balance between a private individual's valid need to secure personal information and law enforcement's ability to access information lawfully is proving difficult. This challenge was highlighted during the FBI's efforts to access the San Bernardino gunman's iPhone in 2016 and continues to be an issue today. Technology companies increasingly offer products with built-in encryption technology that prevent access to data, even from law enforcement entities with a warrant. As one example, the FBI was unable to access approximately 7,500 mobile devices submitted to its Computer Analysis and Response Team over the last year, even though there was legal authority to do so. Malicious actors continue to use new technology advances to evade law enforcement efforts. To continue to counter this threat, the FBI requested nearly $22 million in its FY 2018 budget request.

Source: FBI

Likewise, the DarkNet presents another challenge for the Department in identifying criminals acting in an anonymous environment. While the DarkNet facilitates anonymity for sensitive communications among individuals such as medical professionals, victims of domestic violence, political dissidents, and whistleblowers, users also include terrorists, organized criminal networks, drug dealers, and child pornographers who take advantage of its anonymity to mask their nefarious activities. Disrupting and dismantling illicit DarkNet activity is both a priority and a challenge for the Department, especially in light of estimates that 80 percent of DarkNet traffic relates to the sexual exploitation of children. In November 2014, a joint FBI and DHS investigation led to the seizure of Silk Road 2.0, a DarkNet website used for illegal drug sales and other illicit activities. At that time, it was one of the most extensive criminal enterprises on the internet, with $8 million in sales a month. More recently, in July 2017, the Department successfully coordinated with international law enforcement partners and other agencies to shut down AlphaBay, the largest illicit DarkNet market at that time.

Finally, although the Department continues to prosecute hackers from around the globe with the help of local, state, and international law enforcement, the global nature of internet and electronic communications highlight the challenges of coordinating with multinational partners—each operating within a different legal system with diverse laws governing the collection of electronic evidence. While the Department has mechanisms to assist in this effort, challenges exist. The United States has mutual legal assistance treaties with less than half of the countries in the world, and some of these partner countries are limited by the type of assistance they can provide and the timeline in which they can respond. The Department also has attempted to obtain access to electronic evidence from U.S. companies that store such data overseas by serving federal search warrants on them, with inconsistent results. For example, the Second Circuit Court of Appeals ruled in 2016 that Microsoft did not have to produce data stored on servers located in Ireland in response to a search warrant issued pursuant to the *Stored Communications Act of 1986* (SCA). However, federal district courts in Pennsylvania and the District of Columbia ruled that a search warrant issued pursuant to the SCA did require Google to disclose all records accessible from its headquarters, even if those records were stored on servers located outside the United States and in October, the Supreme Court granted the Department's petition for a writ of certiorari from the Second Circuit's decision in the Microsoft case. The Department

must find a way to close the gaps in legal authorities used to prosecute cyber criminals, strike a balance between protecting citizens' privacy while protecting them from cybercrime, and improve coordination with friendly foreign governments to prosecute foreign cyber criminals.

Preparing the Department for Cyber Threats

The Department has designated cybersecurity as a top priority in its FY 2014-2018 Strategic Plan and committed additional resources to address the issue. The Department's FY 2018 budget requests $30.9 million and 34 authorized positions for its information technology (IT) resources, including major investments in IT modernization, cybersecurity, and information sharing technology.

OIG Report: Cybersecurity Logical Access Controls and Data Security Management Practices

In an August 2016 report, the OIG found that significant work is still needed in implementing personal identity verification cards to authenticate and grant access to users of the Department's IT systems.

Also in its FY 2018 IT budget request, the Department acknowledged that the Justice Security Operations Center, which provides 24/7 monitoring of the Department's internet gateways and incident response management, is hampered by its aging infrastructure, some of which is past its end of useful life and is no longer supported. In addition, the Department's IT budget request provides funding to enhance its insider threat efforts by improving its continuous monitoring of user activities on the Department's IT systems and its proactive analysis of the same for suspicious activities. It is important that the Department make IT acquisitions as expeditiously as possible and leverage private sector technology when possible while respecting the privacy rights of those affected by the new systems.

To address the challenge of increasing cyber threats, the FBI's FY 2018 budget request includes an enhancement of $41.5 million and 36 positions in support of these efforts. In a June 2017 statement before the House Appropriations Committee, then-FBI Acting Director Andrew McCabe stated that "virtually every national security threat and crime problem the FBI faces is cyber-based or facilitated." He further stated that the FBI is engaged in a wide range of efforts to identify cyber threats, including sharing threat information inside and outside of government and developing and retaining an adequate cyber workforce to evolve and address the rapidly growing cyber threat, as discussed in more detail in the *Human Capital* section of this report.

Managing an Overcrowded Federal Prison System in an Era of Declining Resources

Despite a declining federal inmate population in recent years, the Department continues to face a number of challenges with the federal prison system. As of mid-April 2017, the federal prison system remained 14 percent above its rated capacity, with high security institutions operating at 25 percent over rated capacity. Further, the BOP projects that the inmate population will increase by about 2 percent in FY 2018 based on the Department's increased enforcement and prosecution efforts. Additionally, the federal inmate population continues to age, resulting in increased costs, particularly for medical care, as noted in a 2015 OIG review. These population changes compound the Department's challenge of weighing BOP's resource needs against those of other Department components and programs.

Operating in an Increasingly Resource-Challenging Environment

Staffing, aging facilities, and tightening budgets present constant challenges for the BOP in carrying out its mission to confine offenders in safe, humane, and cost-efficient environments. Across the federal government, agencies are facing flat or declining budgets, and, earlier this year, the Office of Management and Budget issued guidance instructing agencies to take immediate actions to achieve workforce reductions and cost savings. The challenge for the Department is managing a federal prison system that over the past 20 years has taken an ever larger share of the Department's budget, currently accounting for nearly 25% of the Department's budget, yet remains overcrowded.

Source: BOP

Staffing challenges are also prevalent at private facilities contracted by the BOP and U.S. Marshals Service (USMS). A December 2016 OIG audit of the BOP's contract with CoreCivic Inc. (CoreCivic) to operate the Adams County Correctional Center in Natchez, Mississippi, found that the facility was being staffed at a lower level than during a 2012 riot that resulted in the death of a correctional officer. The OIG also audited the USMS's contract with CoreCivic to operate the Leavenworth Detention Center, and found that vacancies led to the closure of security posts and reassignment of personnel, to the detriment of detainee services. And, in August 2016, an 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. In February 2017, the Department announced its intention to continue to use private prisons to house federal inmates. The BOP and the Department face the challenge of effectively overseeing these private prisons, and ensuring that they are providing the level of staffing, security, and programs that the contracts require.

BOP resource constraints also affect existing and proposed institutions. In its FY 2018 congressional budget request, the Department rescinded funds for construction of a new U.S. Penitentiary in Letcher County, Kentucky—a decision which the Deputy Attorney General explained was a tough budget choice. GAO has identified as a key issue BOP's deferred maintenance of its facilities, which contributes to the continued deterioration of its aging infrastructure. In FY 2017, the BOP had a backlog of major facility modernization and repair projects totaling $542 million, representing a 58-percent increase since FY 2014. However,

unforeseen emergency repairs impact BOP's ability to reduce this backlog. For example, the BOP allocated $8.2 million for emergency repairs at the Federal Correctional Institution in Aliceville, Alabama, after it was damaged by a tornado in February 2016. This backlog may be further exacerbated in FY 2018 from damage to BOP facilities in regions affected by the active 2017 hurricane season.

Considering the Impact of New Immigration Enforcement and Sentencing Policies

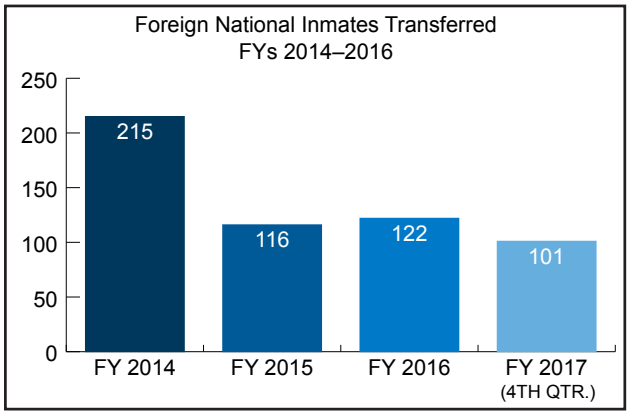
In 2017, the Department issued immigration enforcement and sentencing policies that may increase the demand on BOP's resources. In April 2017, as part of the Department's efforts towards criminal immigration enforcement, the Attorney General announced a new immigration policy that encouraged prosecutors to seek felony charges and pursue mandatory minimum sentences for immigration-related offenses. Further, in May 2017, the Attorney General established charging and sentencing policies that directed prosecutors to charge and pursue the most serious, readily provable offenses. Some of these offenses carry mandatory minimum sentences, which the U.S. Sentencing Commission (USSC) found to carry an average minimum sentence of 110 months of imprisonment. The Department will need to monitor the impact of these policies on its federal prison population and assess the capacity and cost of private prisons and detention centers, particularly those that house foreign national inmates and detainees.

Evaluating the Effectiveness of Ongoing Efforts to Reduce Inmate Population and Recidivism

Challenges associated with tightening resources and new policies heighten the Department's need to evaluate the outcomes of ongoing programs that seek to reduce the inmate population and recidivism. In FY 2015, the BOP spent $360 million on residential reentry centers (RRC) and home confinement costs and reported to have 181 RRCs operated by 103 different contractors as of September 2016. However, a November 2016 OIG report found that the BOP does not have performance measures to evaluate the effectiveness of its RRC and home confinement programming, nor procedures that adequately assess services provided by RRC contractors. In a June 2017 report, the OIG found that, at one RRC, inmate program plans did not establish goals that addressed inmate's top risk areas, nor did staff consistently document inmate progress toward achieving program plan goals.

The Department would also benefit from measuring the outcomes of sentencing alternatives such as pretrial diversion programs, which divert qualified offenders from the traditional criminal justice process into a program of supervision and services. In a July 2016 report, the OIG found that neither the Executive Office for U.S. Attorneys nor the U.S. Attorney's Offices track metrics for evaluating a program's effectiveness, such as the total number of offenders who were placed in a program or the total number of unsuccessful participants. The OIG also reported that the Department did not evaluate the potential for diversion programs to reduce prosecution costs, incarceration costs, or recidivism.

Two programs that can potentially reduce overcrowding in the federal prison system and yield cost savings are the Department's Compassionate Release and International Prisoner Transfer Programs. A 2016 USSC amendment aimed at increasing the use of compassionate release broadened eligibility criteria for inmates when "extraordinary and compelling reasons" exist. In May 2015, an OIG report recommended that the BOP consider revising its compassionate release policy and, as of September 2017, that recommendation remains open. From the start of FY 2016 through July 6, 2017, the BOP received 1,560 requests for compassionate



Source: OIG analysis of DOJ information

release; however, the BOP granted compassionate release to just 114 inmates during that same time period. The Senate Appropriations Committee's report accompanying the Senate draft of the FY 2018 appropriations bill for the Department directs the BOP to report to the Committee on the steps BOP has taken to implement the OIG and USSC's recommendations, and for those recommendations not met, BOP's plan for meeting them or reasons why they cannot be implemented. Through the International Prisoner Transfer Program, the Department is able to reduce its prison population by transferring foreign national inmates to their home countries to complete their sentences. However, despite the Department's efforts to encourage treaty nations to accept more inmates, the number of foreign nationals transferred to treaty nations declined in FY 2017 when compared with the prior 3 years.

The Department tracks some data on the cost implications of using incarceration alternatives. By taking steps to obtain outcome data and developing performance measures for these alternatives, the Department and BOP will be better positioned to determine the extent to which the alternatives are achieving their goals and objectives and what adjustments may be necessary to make them more effective.

Strengthening the Relationships Between Law Enforcement and Local Communities and Promoting Public Trust

Strengthening police-community relationships, compiling accurate data on use of force by law enforcement officers nationwide, and ensuring proper oversight of its own law enforcement officials are a priority for the Department, especially in light of recent events around the country that have underscored the need for enhanced collaboration between the Department, law enforcement agencies, and the community.

Source: DOJ

Strengthening the Relationship Between Law Enforcement and the Community

Recent high-profile police misconduct incidents, while not representative of police conduct nationwide, have nevertheless emphasized the need to strengthen and sustain police community relationships. The Civil Rights Division (CRT) and the Community Oriented Policing Service (COPS Office) serve critical, yet distinct roles in accomplishing police reform and improving police-community relations. Pursuant to federal law, CRT reviews the practices of law enforcement agencies that may be violating people's federal rights, including cases involving allegations of use of excessive force; unlawful stops, searches, or arrests; and discriminatory policing. Since 1997, the CRT has entered into 40 reform agreements; 20 court-enforced consent decrees; and 20 settlement agreements with local law enforcement agencies. These agreements and consent decrees guide reforms at law enforcement agencies, with the goal of increasing community confidence in law enforcement.

In addition to the CRT's investigations of law enforcement agencies to determine whether there is evidence of an agency engaging in a pattern or practice to violate people's rights, the Department has a number of other tools for establishing police-community trust, including the COPS Office's Critical Response initiative and its Collaborative Reform Initiative for Technical Assistance (CRI-TA). The Critical Response initiative assists law enforcement agencies in dealing with high-profile events and major incidents that could create tension and conflict in the community. CRI-TA was created in 2011 and historically allowed law enforcement agencies to request technical assistance to help them identify issues that might impact public trust, such as use of force, racial profiling, and other misconduct. CRI-TA attempted to resolve these concerns by conducting an investigation and issuing publicly available recommendations for improvement to the participating law enforcement agencies. In September 2017, the Department announced significant changes to CRI-TA. As a result of the changes, moving forward CRI-TA will continue to focus on providing targeted technical assistance in the areas of public safety and crime reduction directly to local law enforcement agencies, based on the needs and requests identified by those agencies. However, CRI-TA will focus resources on technical assistance and support, rather than on investigative assessments. As these programs are voluntary, a challenge for the Department is increasing these partnerships with law enforcement agencies around the nation to address concerns of misconduct and mistrust of law enforcement among communities.

In a March 2017 memorandum, the Attorney General also initiated a review of "all Department activities—including collaborative investigations and prosecutions, grant making, technical assistance and training, compliance reviews, existing or contemplated consent decrees, and task force participation" associated with supporting state and local law enforcement agencies. A challenge for the Department will be

managing the transition for all impacted programs to ensure the Department continues supporting its state and local law enforcement partners, while also achieving the strategic goals and principles outlined in the Attorney General's memorandum.

Collection of Use of Force Data

Comprehensive data on the use of excessive or deadly force by law enforcement is necessary for an informed discussion about relations between law enforcement and communities. Historically, the Department has struggled to compile complete and accurate data due to its reliance on voluntary reporting and the variation in the methods used to collect information by different states. Collection of this data is mandated by both the *Violent Crime Control and Law Enforcement Act of 1994*, which requires the Department to collect and report "about the use of excessive force by law enforcement officers," and the *Death in Custody Reporting Act of 2013* (DCRA), which requires federal and state law enforcement agencies to report any deaths of individuals that occurred during interactions with law enforcement while in their custody. DCRA authorizes the Department to impose grant funding reductions if states do not submit data, but there is no mandate for states to submit non-lethal use of force data. To close this gap, the Department began partnering with local, state, tribal, and other federal law enforcement to enable nationwide collection of use of force data. In December 2016, the Department released plans to improve DCRA data collection, and will begin collecting quarterly data from states pursuant to DCRA reporting guidelines in the third quarter of 2017.

In early 2016, the FBI initiated a project to collect data on police use-of-force that results in death or serious bodily injury, as well as shooting incidents. On July 1, 2017, the FBI began a 6-month pilot study to evaluate data quality and completeness from participating agencies, which include the Department's law enforcement components and local, state, and tribal law enforcement agencies and organizations that have volunteered to contribute data. The FBI expects to begin bulk data collection in early 2018 and has created an internet-based data portal to receive the data. As these data collection sources continue to develop, the Department's challenge is to ensure quality data is organized and analyzed consistently to better understand police use of force trends, and to help local, state and federal law enforcement find creative solutions based on this information.

Practicing Proper Oversight of Law Enforcement Personnel to Ensure Public Trust

Robust oversight of federal law enforcement programs is necessary to ensure public confidence in their effective and efficient operation. Inadequate oversight increases the risk of unlawful conduct by law enforcement personnel, can compromise the integrity of Department actions, may imperil efficient and effective use of taxpayer funds, and can leave U.S. citizens vulnerable to civil rights violations. For example, the OIG's 2017 report on the Department's oversight of cash seizure and forfeiture activities identified flaws in both training and oversight of asset forfeiture, which compromised the Department's ability to ensure that seizure and forfeiture activities advance criminal investigations and do not present a potential risk to civil liberties. The review found many seizures for which no discernible connection between the seizure and the advancement of law enforcement efforts could be identified. Due to the risks inherent in the practice, and a July 2017 directive increasing the Department's ability to conduct seizures, it will be a challenge for the Department to ensure appropriate training and oversight in this area.

OIG Review: ATF's Controls over Agent Cashier Funds

The OIG is currently assessing the ATF's controls over agent cashier funds, which are used to facilitate the purchase of evidence, procurement of services, and payment for information related to criminal investigations.

A lack of oversight also has the potential to compromise the integrity of Department investigations, contribute to the ineffective and potentially wasteful use of taxpayer funds, and affect compliance with

Fourth Amendment protections. For example, the OIG's 2016 audit of the DEA's management and oversight of its confidential source program identified significant deficiencies in the DEA's operation and supervision of its program, including that the DEA did not adequately oversee payments to its sources. The OIG also found that the DEA "reactivated" a previously deactivated confidential source known to provide false testimony in trials and depositions. During the approximate 5-year period of reactivation, this source was used by 13 DEA field offices and paid $469,158; over $61,000 of that amount was paid after this source was once again deactivated for making false statements to a prosecutor.

Additionally, the OIG released a joint report with the Department of State OIG on responses by the DEA and Department of State regarding three deadly use of force incidents in Honduras. The report found significant oversight issues specifically pertaining to incident planning; post-investigative review efforts; and factual misrepresentations of overseas operations to the public, Department leadership, and Congress. As demonstrated by these incidents, ensuring adequate oversight and accountability measures remains a top concern and challenge for the Department.

Coordinating Within the Department and Across Government to Fulfill the Department's Mission to Combat Crime

Coordinating with federal, state, local, and tribal communities to address the most pressing national criminal justice issues remains a high priority for the Department. The men and women of the Department's law enforcement components are tasked with critically important responsibilities, including protecting the public from violent crime and the illegal trafficking of drugs, and promoting collaboration between law enforcement agencies in order to safeguard the American public and ensure mission success. While the Department continues to operate as a leader in law enforcement, an array of challenges persists.

Promoting and Ensuring Efficient Agency Coordination

With limited government resources, it is essential for law enforcement components to coordinate resources efficiently to ensure mission success. For decades, the Department's law enforcement components have led and supported numerous task forces—including the Organized Crime Drug Enforcement Task Forces, the High Intensity Drug Trafficking Area Task Forces, the Joint Terrorism Task Forces, and the Internet Crimes Against Children Task Forces—all of which enable the Department's law enforcement components to collaborate with each other, as well as with other federal, state, and local law enforcement partners, to leverage resources and expertise in the Department's continuous fight to combat crime and terrorism.

OIG Reviews: Coordination with Law Enforcement Agencies

The OIG is currently assessing the coordination between the Department and DHS law enforcement components in conducting criminal investigations along the U.S. Southwest border. In addition, the OIG is assessing the Department's law enforcement activities and responsibilities pursuant to the *Tribal Law and Order Act of 2010*, including legal assistance, investigative training, and other technical assistance used to enhance law enforcement efforts in Indian Country.

There is, however, continued room for improvement for the Department in this area. For example, the OIG's 2017 review of the El Paso Intelligence Center (EPIC)—a DEA-led, multi-agency center with a mission of supporting law enforcement through the timely, coordinated analysis and dissemination of intelligence on the illegal activities of organizations and threats to the nation—found that the leaders of the DEA's partner agencies have not been effectively engaged in governing the center because they have not been sufficiently involved in defining its strategic priorities and monitoring its operations and performance. Further, the OIG found that the DEA has supported two similar programs, one at EPIC and one at the DEA Houston Field Division, which both collect the same type of real-time tactical intelligence along different parts of the Southwest border. These programs have operated independently, and generally have not shared collected information with one another. As a result, the DEA may not realize the full value of the intelligence it collects to identify trends and patterns of criminal activity all along the Southwest border, nor the potential cost savings that could possibly be realized through the consolidation of these similar programs. The problems identified by the OIG's EPIC review demonstrate that effective and efficient coordination among law enforcement components continues to pose a challenge for the Department.

Additionally, in January 2017, the OIG released its audit of the Office of Justice Programs' (OJP) Tribal Justice Systems Infrastructure Program (TJSIP), which identified coordination deficiencies between OJP and the Bureau of Indian Affairs (BIA) that resulted in three TJSIP-funded correctional facilities that could not be opened, or could only be partially opened, due to construction flaws or operations and maintenance

funding issues involving BIA. These three facilities, which together cost nearly $22 million, remained non-operational or partially operational for over a decade after the initial awards were made, and for 3 or more years after the TJSIP grants were fully expended. In both cases, the lack of effective agency coordination impedes the Department's ability to effectively address tribal and border public safety issues and compromises its ability to make use of taxpayer funds effectively. The Department has made efforts to improve coordination and information sharing, including greater information sharing with tribal partners and the establishment of collection initiatives and programs to share information between DEA and its federal partner agencies. Additionally, in November 2017, the Attorney General announced the creation of the Violent Crime Reduction Coordinating Committee that will coordinate violent crime reduction efforts across the department, as well as serve to institutionalize these efforts to help ensure continuity and durability over time. However, to promote public safety and ensure that taxpayer funds are spent with the utmost integrity, efficient agency coordination must remain a top priority.

Violent Crime

From the early 1990s through 2015, the violent crime rate in the United States fell 50 percent. However, in September 2017, the FBI released semiannual crime statistics for 2016 showing an overall increase in the number of violent crimes reported in 2016 when compared with 2015. These crimes included murder, non-negligent manslaughter, rape, aggravated assault, and robbery. Violent crime in cities with a population over 1 million increased over the previous year by 7.2 percent. Smaller cities with a population over 25,000, but under 1 million, saw increases in violent crime between 3.3 and 5.8 percent. The Department's FY 2018 budget requests $198.5 million to: (1) reduce violent crime; (2) target Transnational Criminal Organizations; and (3) combat the prescription drug and opioid epidemic. This funding was requested to augment a wide-ranging set of Department programs that seek to leverage law enforcement operations, prosecutorial action, and support for state and local governments that contribute to the Department's initiatives to reduce violent crime and protect our communities by apprehending violent criminals.

OIG Review: Violent Crime

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.

A continuing challenge for the Department is to identify ways to best support state and local law enforcement agencies and prosecutors with limited resources to stem the uptick in violent crimes. In June 2017, the Attorney General announced the creation of the National Public Safety Partnership to lead a national effort to combat violent crime and provide a framework to assist state, local, and tribal law enforcement officials in effectively investigating violent crimes and pursuing those involved in gun crime, drug trafficking, and gang violence. In October 2017, the Attorney General announced the reinvigoration of Project Safe Neighborhoods (PSN), a program designed to bring together all levels of law enforcement and community stakeholders to provide a comprehensive approach to violent crime reduction—one that includes prevention, enforcement, and reentry efforts, as well as criminal investigations and prosecutions. Each U.S. Attorney must implement a PSN plan as part of the newly revived initiative. The Department has also partnered with local law enforcement agencies to investigate and prosecute top-level leaders of Mara Salvatrucha, otherwise known as MS-13, a transnational criminal gang responsible for committing violent crimes. For example, the FBI's Long Island Gang Task Force includes FBI agents and officers from state and local law enforcement agencies, all of whom work together to investigate and apprehend suspected MS-13 operatives. According to New York's Suffolk County Police Commissioner Timothy Sini, because of MS-13's transnational reach, successful investigation and prosecution strategies require collaboration across jurisdictions to gather and share meaningful intelligence.

Opioid Epidemic and Drug-Related Crime

OIG Review: DEA's Opioid Enforcement Efforts

The OIG is conducting a review to assess whether the DEA's regulatory activities and enforcement efforts effectively prevent the diversion of controlled substances, particularly opioids, to unauthorized users. Specifically, this review will examine: (1) the DEA's enforcement policies and procedures to regulate registrants; (2) the DEA's use of enforcement actions involving distributors of opioids who violate these policies and procedures; and (3) the DEA's coordination with state and local partners in countering illicit opioid distribution.

The Attorney General recently described the opioid epidemic as a crisis for law enforcement which has contributed to the recent surge of violent crime in America. In August 2017, the Attorney General announced the creation of the Opioid Fraud and Abuse Detection Unit, a new Department data analytics program focused on identifying opioid-related health care fraud. In addition, the DEA has initiated outreach to Native American communities, which face high rates of opioid-related deaths, regarding access to federal crime data on opioids. According to the DEA, drug overdose deaths are at an all-time high and have outnumbered deaths by firearms, motor vehicle crashes, suicide, and homicide since 2009. Given the opioid epidemic and the resulting increases in drug-related crime, incarcerations, and overdose deaths, the Department's challenge is not only to enforce the nation's drug laws, but to also collaborate with state and local law enforcement and public health services in addressing the crisis.

As our nation's law enforcement agencies continue to battle this crisis, the introduction of synthetic opioids presents an additional threat. Of particular concern is the synthetic opioid fentanyl; even minute amounts of the drug are lethal, and can be inadvertently inhaled, presenting serious risks to both drug consumers and law enforcement personnel. Law enforcement officials report higher availability and increased seizures of fentanyl, and more overdose deaths from fentanyl than at any other time since the creation of these drugs in 1959. Between 2014 and 2015, deaths attributed to fentanyl increased by 72 percent, and affected all demographics and regions of the country.

The Department funds numerous programs that partner with local law enforcement and public health agencies to stem drug abuse, misuse, and diversion at the source. For example, in September 2016, the Bureau of Justice Assistance (BJA) awarded $8.8 million to state health and pharmacy departments to compile and share prescription drug information through the creation of state-run Prescription Drug Monitoring Programs. In September 2017, BJA awarded approximately $24 million in federal grants to 50 cities, counties, and public health departments to provide financial and technical assistance to state, local, and tribal governments to create comprehensive diversion and alternatives to incarceration programs for those impacted by the opioid epidemic. In addition, the DEA's 360 Strategy coordinates with state and local law enforcement to target and prosecute drug traffickers; engages with drug manufacturers, pharmacies, and practitioners to prevent the misuse of prescription drugs; and partners with local communities to prevent drug and violent crime issues from resurfacing. As these and other programs demonstrate, the magnitude of the opioid epidemic means that the Department must take a comprehensive approach that focuses not only on enforcement, but also providing funding for programs that address prevention and treatment. As the opioid crisis continues, the Department's challenge will be to strengthen its partnerships with state and local communities to address the epidemic in communities throughout the country.

Administering and Overseeing Contracts and Grants

The Department continues to face challenges in the administration and oversight of its contracts and grants; these challenges create a heightened risk of fraud, waste and mismanagement. As the Department relies more on the use of contracts and the awarding of grants to fulfill its mission, it becomes increasingly important for it to develop the expertise necessary to administer contracts and its grant programs efficiently, effectively, and in accordance with both federal regulations and Department policy. In FY 2017, the Department reported that it awarded almost $7.4 billion in contracts and had over $3.5 billion available for grants and cooperative agreements. Given the resources involved, the Department must continue to improve its management of its contracts and grant programs.

Contracts

The Department contracts for a wide variety of goods and services, including legal support services, inmate healthcare, and IT equipment. Despite the diversity of the Department's contracts, the OIG has found some issues that are consistent among them, including insufficient oversight of some of the Department's contracts and the failure to comply with the Federal Acquisition Regulation (FAR) throughout the procurement process.

Source: OIG

Proper oversight is necessary to ensure that the Department is receiving the appropriate goods or services, the contractor is submitting only valid and accurate invoices, and the contractor is complying with the terms and conditions of the contract. However, human capital constraints, decentralized contracting functions, and a lack of adequate monitoring frameworks, such as training and formal policies, often impede the Department's oversight of contractors. For example, as discussed in the *Prisons* challenge, the OIG recently completed an audit of a contract to CoreCivic to operate the Leavenworth Detention Center and identified significant shortcomings in the USMS oversight of the contract that had a total estimated value of $697 million. The audit also found that the USMS Contracting Officer's Representative, who was responsible for monitoring CoreCivic's performance on a day-to-day basis, was located offsite, had no previous contract oversight experience, and received no formal guidance and negligible detention-related training.

The Department's challenges in providing oversight of its contracts are of particular concern, given that, in FY 2017, 27 percent (or $1.95 billion) of its contracts were time and material (T&M) and labor-hour contract awards. T&M and labor-hour contracts are considered to be high risk contract types because they provide no incentive for the contractor to control cost. As a result, these contracts require greater government oversight and may only be used when it is impossible to estimate accurately the cost, extent, or duration of the work, at the time of contracting, and no other contract type is suitable.

As stated earlier, the Department also has challenges in complying with the FAR throughout the procurement process. For example, in a July 2017 audit of the FBI's lease of executive aircraft, the OIG identified several deficiencies, including non-compliance with the FAR. Specifically, the FBI violated the FAR by not obtaining the proper approval for its sole source justification prior to the award of the contract. Further, the FBI did not formally award the contract until approximately 1 month after the period of performance

began. In addition to the weaknesses we identified with the FBI's actions in awarding the lease extension, we also identified weaknesses with the FBI's execution of its contract administration responsibilities. The OIG also determined that the FBI did not: (1) adequately review invoices; (2) pay invoices in a timely manner; (3) maintain sufficient documentation in the contract file to show a complete history of the contract action; or (4) enter accurate information into the Federal Procurement Data System—all of which are in non-compliance with the FAR. These OIG audits highlight the challenge facing the Department in ensuring that contracting officials understand the extent of their responsibilities regarding the laws and regulations surrounding contract administration and oversight.

Grants

The Department, with a total active grant portfolio of $12 billion through 11,000 awards, faces challenges in both grant management and oversight. OIG audits have consistently identified instances in which the Department was unable to ensure adequate performance by grantees and sub-grantees. Specifically, our audits have identified the following findings and deficiencies: the failure to demonstrate progress toward achieving the awards' stated goals and objectives; non-compliance with essential award conditions related to performance reports, use of funds, drawdowns, and contract management; and weaknesses and deficiencies in the areas of internal control environment, expenditures, matching, budget management, monitoring of contractors, reporting, and program performance and accomplishments.

In prior years' Top Management and Performance Challenges reports, we highlighted the increased responsibility the Department faces in its management of the Crime Victims Fund (CVF), due to significant funding increases provided to recipients. CVF awards, which primarily fund formula grants to states and territories to support compensation and services for victims of crime, continue to present significant management challenges as the program funding increases. The $2.36 billion available in FY 2015 for CVF distributions more than tripled the FY 2014 funding, and sustained levels above that figure for FYs 2016 and 2017 increase this challenge. We have a continuing concern that the Department, state administering agencies, and recipients do not yet have the proper controls in place to oversee the large influx of funding. For example, in a September 2017 OIG audit, we identified areas of risk for which the Office for Victims of Crimes' (OVC) management of CVF grant programs should be strengthened. Specifically, we found improvements were necessary regarding the frequency and adequacy of OVC monitoring efforts. Additionally, our audit found risks associated with the OJP staff's understanding and performance of grant recipient monitoring procedures. We also identified risks associated with OJP's performance measures for CVF-funded activities.

OIG Reports: Crime Victims Fund

As part of the FY 2015, 2016, and 2017 appropriations, $10 million in CVF funding was provided each year to the OIG for increased oversight and auditing activities associated with the anticipated increases in both funds available, and in the number of grant recipients. From January 2016 through September 2017, OIG has issued 18 CVF audits that identified approximately $2.5 million in questioned costs and numerous concerns about various state governments' management of these funds including conflicts of interest and unallowable costs.

We will continue our oversight of programs funded by the CVF and to recommend improvements for the Department and grantees to best ensure that the use of CVF funds results in effective services for victims of crime.

In addition, in July 2017, the OIG completed an audit of the Office of Juvenile Justice and Delinquency Prevention's Title II Part B Formula Grant Program, which supports local and state efforts to prevent juvenile delinquency and improve the juvenile justice system through grants. The report found that OJJDP failed to ensure compliance with the core requirements of the *Juvenile Justice and Delinquency Prevention Act*.

Specifically, we determined that OJJDP did not routinely perform audits of states that received grants in order to assure compliance with the Act, as required under federal regulations, nor did they have written policies and procedures for state audit selections. The report's findings highlight the Department's ongoing challenge to ensure that its oversight of its grant programs is effective.

Using Performance-Based Management to Improve Department Programs

Performance-based management continues to be a significant challenge for the Department, with many components lacking the ability to effectively collect, verify, or analyze performance data related to their programs. From BOP's healthcare and rehabilitation services to DEA and ATF's confidential informant programs, the OIG's reviews have found that the Department often lacks the data and analysis necessary to ensure that its resources are used efficiently and effectively. Performance-based management is crucial both to understanding the impact of the Department's programs and to proactively identifying areas of risk.

Collecting, Verifying, and Analyzing the Right Data

Performance-based management includes the ongoing monitoring and reporting of program accomplishments, particularly progress towards pre-established performance goals. During the last decade, the federal government enacted new data standards and reporting requirements in an effort to improve the transparency and quality of federal data. As of May 2017, all federal executive agencies must report spending data using the standardized data structure established by the *Digital Accountability and Transparency Act of 2014* (DATA Act). The OIG's December 2016 DATA Act review found that the Department was on track to implement these reporting requirements by the May 2017 deadline. Additionally, the *Government Performance and Results Modernization Act of 2010* requires agencies to publicly report their progress towards meeting specified performance goals—though a June 2017 OMB memorandum temporarily suspended these reporting requirements until new performance goals are established under the President's FY 2019 budget. Standardized data provides new insights into agency spending patterns and performance, as well as enables the use of government-wide data analytics to fight fraud, waste, and abuse.

Despite the legislative requirements to collect and report on performance data, the Department still faces the challenge of how to collect the right data, verify that the information is accurate and reliable, and effectively analyze the data to determine the outcomes of its programs.

Measuring Program Effectiveness

A key challenge for the Department is using performance data properly to ensure that its programs meet policy goals and to use that information to inform future strategy. Historically, the Department has struggled to acquire and leverage available data to measure program effectiveness and implement necessary programmatic changes. For example, the OIG's review of the BOP's management of inmates in RRCs and home confinement found that the BOP lacked performance measures to gauge both the success of these programs in helping inmates transition back into society and the quality of services that contractors provided to inmates. Similarly, a July 2016 OIG review found that the Department does not evaluate the effectiveness of its pretrial diversion programs or their potential to reduce prosecution or incarceration costs. Analyzing data to determine inmate risk and efficacy of service delivery could help the Department more effectively manage and serve its inmate population.

Proper performance analysis can identify both program successes and areas for improvement. For example, a June 2017 GAO review found that the FBI Laboratory has a strong performance management process to ensure reliability and quality in forensic examinations of chemical and trace evidence. On the other hand, as discussed in the *Contracts and Grants* section, OIG audits have identified instances in which Department grantees and contractors are unable to provide sufficient support for their use of federal funds or verify their performance of program objectives. For example, OIG's September 2017 audit of OJP's management

of CVF grant programs found that OJP's performance measures were not outcome-oriented and could not be used to assess the impact of the programs or the quality of services provided to victims. Similarly, while a goal of the Department is to strengthen communities and their relationship with law enforcement, the Department often lacks the performance measures to ensure that its law enforcement operations and programs meet this goal. Performance-based management can help the Department identify best practices for achieving its strategic goals and objectives.

Identifying Areas of Risk

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. For example, the OIG's reviews of the ATF and DEA confidential source programs found that confidential informant payment information was not sufficiently tracked, recorded, or evaluated. During our September 2016 review, we found that the DEA made payments of $25 million to 9 sources over a 5-year period and $30 million to 1 source over a 30-year period, all without independently validating the reliability of the sources or the accuracy of their information. The OIG's July 2017 review of a $2.4 million aircraft lease contract awarded by the FBI found that the contract did not include specific performance metrics and the aircraft was unavailable for about one quarter of the lease period. Effective tracking and analysis of performance data could enable Department components to detect anomalies or other concerns well before millions of taxpayer dollars are spent.

Without evaluating the benefits and risks associated with its programs, the Department runs the risk of funding programs or policies that are ineffective, inefficient, or infringe on the rights of those it is meant to protect. For example, the OIG's review of the BOP's use of restrictive housing for inmates with mental illness found that the BOP could neither accurately determine the number of inmates who have mental illness, nor ensure that it provided the appropriate care to these individuals. The OIG's March 2017 review of the Department's cash seizure and forfeiture activities found that the Department's investigative components do not use aggregate data to fully evaluate and oversee seizure operations, or the extent to which they may pose potential risks to civil liberties.

Collecting, verifying, and analyzing the right data continues to be a challenge for the Department. As discussed in the *Strengthening Relationships Between Law Enforcement and the Local Community* section, without comprehensive FBI crime data, the Department is constrained in its efforts to address a problem—namely, reduction of violent crime—that it cannot accurately measure or analyze. Similarly, without performance data to measure the effectiveness and efficiency of its programs, the Department will continue to fund programs without fully understanding their outcomes.

Filling Mission Critical Positions Despite Competition for Highly-Skilled Professionals and Delays in the Onboarding Process

To meet 21st century challenges, 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.

Skilled Experts in the Cybersecurity and Healthcare Fields are in High Demand and the Department Struggles to Compete

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 have increased dramatically in the past decade and are expected to continue to grow. Cyber professionals are in high-demand in the private sector, putting the federal government at a competitive disadvantage in the recruitment of individuals with specialized IT skills. The FBI's FY 2018 budget request, for example, included a request for 36 additional cybersecurity-focused positions and for $41.5 million to enhance cyber investigative capabilities. Moreover, in May 2017, the President issued Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, which tasked various federal agencies with developing a plan to bolster the cybersecurity workforce.

A chief 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. As the OIG noted in a July 2015 report, the FBI has struggled to attract computer scientists mainly due to low pay. In addition, in March 2017, the FBI Director remarked that, to attract the best talent in cybersecurity, the FBI needed to explore the possibility of re-hiring former FBI agents who left the Bureau for positions in the private sector.

The Department also faces significant challenges recruiting and retaining medical professionals due, in large part, to competition from the private sector, which offers higher pay and benefits. A March 2016 OIG report found that only 83 percent of the positions in the BOP health services units were filled as of September 2014. As a result, our report noted that inmates were sent to other facilities to receive medical care, further contributing to increased medical costs. The OIG found that the salaries and incentives offered by the BOP were not competitive with those of the private sector, particularly given the need for the BOP to compensate its employees for the safety and security factors intrinsic to working in a correctional facility. The remote locations of many of the prisons pose another challenge to the recruitment of medical personnel to the BOP. Moreover, in our July 2017 review of the BOP's use of restrictive housing for inmates with mental illness, we found that the BOP faced challenges in recruiting and retaining psychiatrists, in particular. As of September 2017, the BOP had filled only 60 percent of its authorized full-time psychiatrist positions nationwide. The Department's ability to attract and retain highly-skilled individuals is critical to helping the Department achieve its mission.

Lengthy Background Investigations Delay the Onboarding of New Personnel

As the rate of federal retirements continues to increase, it is imperative that the Department identifies and hires the most qualified personnel 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 unswerving loyalty to the United States. Delays in completing background investigations for prospective employees could result in delays in the Department's operations. As noted in last year's Top Management and Performance Challenges report, the Department has unique hiring needs and onboarding personnel for certain mission critical positions, such as attorneys, criminal investigators, IT specialists, and legal assistants, can take more than 5 months. Further, many of the Department's mission critical positions also require National Security Information clearances, which can add time to the onboarding process. According to the *2004 Intelligence Reform and Terrorism Prevention Act*, agencies that are authorized to grant National Security Information clearances should complete at least 90 percent of clearances within an average of 60 days. The Office of the Director of National Intelligence's most recent annual report on Security Clearance Determinations noted that the Department continues to experience difficulties in meeting this benchmark of 60 days.

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 create efficiencies in the background check process and improve on-boarding time, particularly for positions deemed mission critical.