U.S Department of Justice

Office of the Inspector General

Top Management and Performance Challenges Facing the Department of Justice - 2019

October 18, 2019

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 2019 report on the 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 reports since 1998. By statute, this report is required to be included in the Department's Agency Financial Report. This year's report identifies eight challenges that we believe represent the most pressing concerns for the Department:

- Managing a Safe, Secure, and Humane Prison System
- Safeguarding National Security and Countering Domestic and International Terrorism
- Protecting the Nation and the Department against Cyber-Related Threats
- Management of Sensitive Investigative Authorities
- Law Enforcement Coordination and Community Engagement
- Administering and Overseeing Contracts and Grants
- Using Performance-Based Management
- Fostering a Diverse, Highly-Skilled Workforce

We believe that managing a safe, secure, and humane prison system is a particular challenge that will garner significant attention in the foreseeable future. Over the last several years, the number of inmates in the Federal Bureau of Prisons (BOP) has declined, so while overcrowding remains a concern, the BOP has an opportunity to address several other issues that can impact both the conditions of confinement for inmates and the work environment for staff. In addition, we identified that enhancing national security and cybersecurity remain key challenges for the Department, particularly given the rising danger of foreign influence operations, which threaten hostile intrusions into the federal government, the American economy, U.S. public discourse, and American elections.

The report also highlights the importance of the Department leveraging diversity and a highly-skilled workforce, as well as using performance-based metrics, to achieve further progress in addressing its most significant challenges. One new challenge identified in this year's report is the need for the Department to effectively manage sensitive investigative authorities, such as the use of confidential sources and surveillance authorized under the Foreign Intelligence Surveillance Act, in a way that safeguards individuals' constitutional and privacy rights and does not undermine public trust and confidence in the Department.

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.

MANAGING A SAFE, SECURE, AND HUMANE PRISON SYSTEM

Source: BOP

Maintaining the safety and security of federal inmates and prison employees remains the overriding challenge for the Federal Bureau of Prisons (BOP). However, the specific aspects of that challenge have evolved. For about 20 years, the BOP was managing operations during a period when the inmate population was consistently and substantially increasing. The total federal prison population was about 40,000 in 1985 and it grew to about 220,000 at its peak in 2013, a roughly 450 percent increase. During that period, the BOP faced significant overcrowding across its institutions. However, over the last several years, the number of federal inmates has declined to roughly 180,000.[1] As a result, while overcrowding and providing appropriate housing for inmates continues to be a challenge at some institutions, several other important issues continue to merit identification as top management and performance challenges for the BOP. These include challenges related to the physical safety and security of inmates and staff, inmate health and welfare, and aging and deteriorating facilities and equipment.

Physical Safety and Security

The BOP faces significant challenges in ensuring the safety and security of prison staff and inmates due to the introduction of contraband into BOP facilities, deficiencies with its security camera system and inmate monitoring, and insufficient staffing.

Contraband. The BOP continues to face challenges preventing contraband, including cell phones, weapons, illegal drugs, and tobacco products, from being introduced into BOP facilities.[2] The OIG is particularly concerned about the challenges to safety and security posed by contraband cell phones. OIG investigations have shown that contraband cell phones in prisons are dangerous weapons. An inmate with a cell phone can carry out criminal activities, including threatening and intimidating witnesses, victims, and BOP staff, and coordinating escape attempts. For example, in 2018, an OIG investigation resulted in a

[1] Recent legislation, such as the passage of the Formerly Incarcerated Reenter Society Transformed Safely Transitioning Every Person Act (First Step Act), and policy actions by the United States Sentencing Commission suggest that this population decline will continue.

[2] Contraband is material prohibited by law, regulation, or policy that can reasonably be expected to cause physical injury or adversely affect the safety, security, or good order of the facility or protection of the public.

BOP inmate being convicted for, among other things, his role in arranging the murder of a BOP correctional officer using a contraband cell phone.

Additionally, the OIG has found that the BOP's attempts to address this challenge are made more complicated by both external and internal threats. External threats include individuals outside of BOP facilities who attempt to smuggle contraband into prisons using drones or the postal system. The BOP has recently experienced an increase in attempts by individuals, acting in concert with persons within the facility, to use drones to drop caches of cell phones and drugs at specifically targeted locations within BOP facilities. In addition, BOP leadership has identified the extensive use of postal mail containing what appears to be innocuous content to introduce synthetic drugs into prisons. OIG audits and evaluations have shown that the BOP has historically struggled to monitor inmates' mail and phone communications effectively, which increases safety risks both within BOP facilities and to the public.

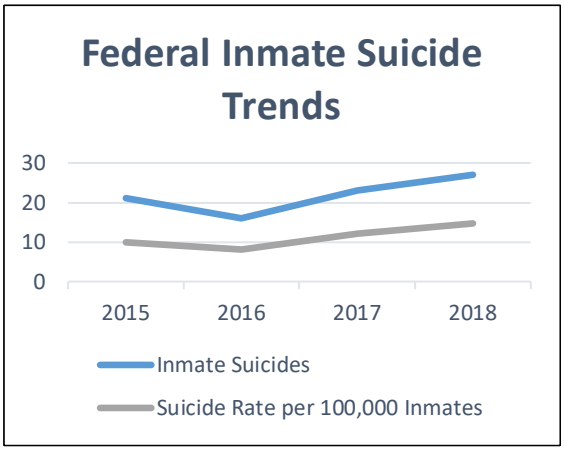
Internal threats, in the form of BOP employees who smuggle contraband into its facilities, further endanger staff and inmates. While only a small fraction of the BOP's approximately 35,000 employees are engaged in introducing contraband, this small group puts both inmates and staff at risk of harm. In 2016, the OIG issued a report on the BOP's policies, procedures, and devices for screening staff, visitors, and inmates for contraband. In the report, the OIG found that the BOP did not effectively implement its staff search policy. Illustrative of the BOP's need for an effectively-implemented staff search policy is a 2019 OIG investigation that found the then chaplain at Federal Correctional Institute (FCI) Berlin in New Hampshire responsible for smuggling significant quantities of contraband, including illegal drugs, cellular telephones, tobacco, and other prohibited items into the prison in exchange for over $52,000 in bribe payments. The now former chaplain was convicted and sentenced to 40 months in prison.

Recently, the BOP has taken steps to address its challenges related to contraband. In 2019, the BOP worked with the National Telecommunications and Information Administration to develop and successfully test micro-jamming devices that can render cellular signals inoperable inside BOP facilities. The BOP should continue its work in this area and assess the feasibility of deploying these devices within BOP facilities. In addition, the BOP should continue its efforts in working with the Federal Aviation Administration to impose flight restrictions over its prisons to thwart drones, and to explore alternatives to the manner in which it handles delivery of postal mail to inmates.

Cameras. In the OIG's 2016 contraband report mentioned above, the OIG found that the BOP's security camera system has known blind spots and poor video quality. Among other things, these video system deficiencies increase the risk of contraband entering BOP facilities. OIG investigations have been hindered, and in some cases, prosecutions of serious crimes within BOP facilities have been precluded because of problems with the BOP's video systems. For example, our 2016 report found that, in multiple instances, the lack of usable BOP video footage was the sole reason that the OIG was unable to

investigate allegations that BOP staff and inmates had introduced contraband into a BOP facility. While the security cameras recommendation remains open, the BOP is taking steps to evaluate and upgrade its security camera system.

Inmate Monitoring. In addition to the issues relating to security cameras, the BOP also faces challenges ensuring that its correctional officers monitor inmates at required frequencies and in accordance with policies to protect inmates, including reducing the risk of inmate homicides and suicides. From FY 2015 through July 2019, the BOP has experienced 46 inmate deaths by homicide and 107 inmate deaths by suicide, including the deaths of high-profile inmates, James "Whitey" Bulger and Jeffrey Epstein. Inmate deaths by suicide in BOP facilities have increased from 8.1 per 100,000 federal inmates in FY 2016 to 14.7 per 100,000 inmates in FY 2018. The OIG is currently investigating several recent inmate homicide and suicide deaths, including those of Bulger and Epstein, to assess any systemic issues that they present, and to ensure that BOP staff are conducting consistent and appropriate monitoring of the inmates in BOP custody to ensure their physical safety.



Source: BOP, OIG

Insufficient Staffing. Although as noted above the BOP's prison population has dropped significantly over the past few years, one of the primary challenges the BOP continues to face is hiring the number of correctional officers it needs to ensure that its facilities remain secure. The BOP has over 35,000 employees to provide care and custody for nearly 180,000 inmates, but projects that it will remain nearly 12 percent understaffed through 2020. To address this staffing shortage, the BOP uses augmentation – assigning individuals other than correctional officers, such as teachers or healthcare professionals – to temporarily fill security posts. The OIG remains concerned that because this practice often places program staff into critical security positions, it interferes with the BOP's ability to ensure the safety of its staff and inmates, as well as its ability to provide inmate programs.

Inmate Welfare

Healthcare staff and contractors, correctional officers, and reentry services workers all have key roles in ensuring inmate welfare. Yet, staffing prisons with qualified healthcare workers is a challenge for the BOP. BOP medical contracts have also led to costs above the Medicare rate and the BOP's health records system makes it difficult for management to assess costs and for investigators to detect fraud.

A 2017 OIG Procedural Reform Recommendation identified that the BOP failed to maintain data of inmate health records electronically and failed to hold its claims adjudication vendor accountable for not performing all contractually required services, including fraud monitoring. The OIG recommended that the BOP require all of its Comprehensive Medical Services contractors to submit electronic claims, ensure those claims are properly analyzed and maintained by the 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. This recommendation remains open.

Healthcare. As discussed in more detail in the *Fostering a Diverse, Highly-Skilled Workforce* section, the BOP faces difficulties in staffing its healthcare provider positions. Nationwide provider shortages, the BOP's inability to provide competitive compensation to providers, and the BOP's rural facility locations each contribute to these difficulties. In addition to the problems of recruiting and retaining qualified healthcare professionals, providing adequate healthcare to inmates remains a challenge for the BOP. As detailed in recent OIG reports, certain characteristics of the BOP's population heighten the challenge of providing proper care for inmates, including aging inmates, inmates with chronic illnesses, and inmates with mental health issues.

The BOP also faces substantial challenges in fulfilling its responsibility to provide inmate health services in an efficient, cost-effective manner. For example, the OIG has found that the BOP has not fully utilized regulatory and legislative tools to help reduce costs while providing adequate care, and has not provided proper administrative oversight for its healthcare functions. In addition to the problem identified in the text box, the OIG issued a 2016 report that found the BOP paid at least $100 million more than the Medicare rate for outside medical care in FY 2014. More recently, a 2019 OIG audit found improper medical payments and a lack of proper approval for pricing in a comprehensive medical services contract.

Reentry Programming. Recidivism reduction remains a major challenge for the Department. A 2016 U.S. Sentencing Commission report found that nearly half of federal offenders released in 2005 were re-arrested within 8 years. Effective reentry programming is an important tool for the BOP to decrease recidivism, and the BOP's FY 2020 budget request calls for $754 million for reentry programming. However, the BOP does not measure the effectiveness of its reentry programs. For example, in a 2016 report on the BOP's Release Preparation Program (RPP), the OIG found that although one of the RPP's objectives is to reduce inmate recidivism, the BOP had no performance metrics to gauge the RPP's impact on recidivism and did not make any attempt to link RPP efforts to recidivism. In addition, in a 2016 report on the BOP's use of Residential Reentry Centers (RRC), the OIG found that the BOP did not have performance measures that evaluate the efficacy of its RRC and home confinement programming, nor did the BOP have procedures in place that adequately assessed the quality of services provided by RRC contractors. In

response to the audit, the BOP developed performance measures to evaluate the efficacy of its RRC program and contractors. However, OIG audits and evaluations of BOP programs have repeatedly identified concerns related to the lack of performance measures that evaluate the efficacy of the programs being reviewed. In this and other contexts, the OIG has urged the Department to use a performance-based management approach to assess the efficacy of its programs. More information on the importance of using performance data to inform Department decision making can be found in the *Performance-Based Management* section of this report.

Infrastructure Issues

The BOP also faces challenges maintaining its aging facilities and equipment. In its FY 2020 Congressional Budget Submission, the BOP notes that many of its facilities and much of its systems/equipment (water, sewer, electrical, and heating/air conditioning) are aged and overused, which causes extensive wear and tear as well as premature deterioration. Our recent work has revealed that even when the BOP is aware of an infrastructure challenge, it does not take timely action to resolve the challenge. For example, in September 2019, the OIG released a review and inspection examining Metropolitan Detention Center (MDC) Brooklyn facilities issues and related impacts on inmates and found that the BOP had been aware of unresolved heating and cooling issues at the facility since at least 2014. Specifically, we found that temperatures in certain housing units dropped below the BOP target temperature of 68 degrees on multiple occasions in January, February, and March 2019. At other times, the temperatures exceeded 80 degrees.

In addition, in its 2015 report on the impact of an aging inmate population on the BOP, the OIG found that the physical infrastructure of BOP institutions cannot adequately house aging inmates. Aging inmates often require lower bunks or handicapped-accessible cells, but overcrowding throughout the BOP system limits these types of living spaces. Aging inmates with limited mobility also encounter difficulties navigating institutions without elevators and with narrow sidewalks or uneven terrain. In the report, the OIG recommended that the BOP study the feasibility of creating units, institutions, or other structures specifically for aging inmates in those institutions with high concentrations of aging inmates. This recommendation remains open.

The OIG is conducting several reviews to assist the BOP in addressing these and other challenges, including reviews of the BOP's policies, procedures, and practices for monitoring communications of inmates with known or suspected ties to domestic and foreign terrorism and its efforts to prevent further radicalization among its inmate population; the BOP's pharmaceutical drug costs for inmates; the BOP's efforts to address inmate-on-staff sexual misconduct; and the DOJ's efforts to protect BOP institutions against the contraband and security threats posed by drones.

SAFEGUARDING NATIONAL SECURITY AND COUNTERING DOMESTIC AND INTERNATIONAL TERRORISM

Enhancing national security and countering terrorism remain top priorities for the Department. In FY 2019, the Federal Bureau of Investigation (FBI) received $5.5 billion to prevent, disrupt, and defeat terrorist operations, prevent and neutralize weapons of mass destruction threats, address cyber threat actors, coordinate counterintelligence activities, facilitate the rapid response to crisis events, and collect intelligence to understand national security and criminal threats. As national security threats continuously change and evolve, so, too, must the Department's approach to combatting those threats. National Security issues relating to *Cybersecurity* and the *Management of Sensitive Investigative Authorities* are discussed in separate challenges below.

Disrupting and Defeating Terrorist Operations

The Department faces challenges in its attempts to disrupt and defeat terrorist operations. According to the FBI, the greatest threat to the Homeland is posed by lone actors, which include homegrown violent extremists (HVEs)—who are inspired by, but not directed by, foreign terrorist organizations (FTOs)—and domestic violent extremists. FTOs, such as the Islamic State of Iraq and ash-Sham (ISIS), also pose a significant threat to U.S. interests at home and abroad.

Both FTOs and lone actors are adept at using the Internet and social media to spread their ideology and attract like-minded extremists. The FBI continues to identify individuals who seek to join the ranks of foreign fighters traveling in support of ISIS, as well as HVEs and domestic violent extremists who aspire to attack the U.S. from within. In its FY 2020 Congressional Budget Submission, the FBI notes that countering the threat of violent extremism is especially challenging for law enforcement because it is difficult to distinguish violent rhetoric from terrorist intent. The OIG is auditing the FBI's efforts to identify HVEs through its counterterrorism assessment process. This audit includes an evaluation of the FBI's coordination with relevant components and its policies and processes to identify and assess HVE threats, as well as a review of the FBI's HVE casework and resource management. The OIG is also conducting an audit of the BOP's counterterrorism efforts. This ongoing work entails a review of the BOP's policies, procedures, and practices for monitoring communications of inmates with known or suspected ties to domestic and foreign terrorism and its efforts to prevent further radicalization among its inmate population.

In FY 2019, the FBI saw an increase in the threat posed by domestic terrorists, which the FBI defines as individuals who commit violent criminal acts in furtherance of ideological goals stemming from domestic influences, such as political, religious, social, racial, or environmental issues. As required by the Attorney General's Guidelines applicable to FBI Domestic Operations, and as the OIG has long noted, the FBI cannot and must not initiate investigations or collect or maintain information based solely on activities protected by the

First Amendment.[3] However, in both the international terrorism and the domestic terrorism realms, distinguishing between First Amendment-protected speech and criminal activity may be particularly difficult in the context of online content or social media posts promoting violence or terrorism.

Counterintelligence and Counterespionage

Preventing and thwarting efforts by our adversaries to collect intelligence information, gather trade secrets, and impact American elections are essential to our national security and remain challenges for the Department. FBI Director Christopher Wray explained in a July 2019 statement before the Senate Appropriations Subcommittee on Commerce, Justice, Science, and Related Agencies, "[f]oreign intelligence services not only seek our nation's state and military secrets, but they also target commercial trade secrets, research and development, and intellectual property, as well as insider information from the federal government, U.S. corporations, and American universities." The nation faces a persistent threat from hostile foreign intelligence services, both through the activities of career foreign intelligence officers and ordinary people, such as students, researchers, or businesspeople operating front companies, who work on behalf of those services. Foreign intelligence services continue to employ increasingly creative and sophisticated methods to steal innovative technology, critical research and development data, and intellectual property in order to erode America's economic leading edge. The FBI must continue its efforts to deter and detect such intrusions and keep pace with the volume and complexity of the methods in its efforts to protect our national security.

Foreign influence operations, which include covert actions by foreign governments to influence U.S. political sentiment or public discourse, also pose a significant national security threat. In addition to using methods like targeting U.S. officials and other U.S. persons through traditional intelligence tradecraft, foreign actors can also use the Internet, social media platforms, and other technology to spread disinformation and escalate divisive issues. We discuss the election security threats the FBI faces, which it must address to effectively defend against future foreign interference in our nation's democratic process, in the *Cybersecurity* section below.

Combatting Insider Threats and Unauthorized Disclosures

To protect itself against insider threats and potential leaks of classified information, the Department must take steps to effectively screen and train personnel, respond appropriately to warning signs, keep pace with evolving technologies, and monitor workplace computer activity. Unauthorized disclosure of classified information can occur either intentionally or unintentionally, both of which present serious national security concerns. As technology advances and encrypted communication options grow, hostile

[3] *See, e.g., A Review of the FBI's Investigations of Certain Advocacy Groups,* September 2010, https://oig.justice.gov/special/s1009r.pdf.

actors with access to sensitive information within an organization by virtue of their employment, as well as those who obtain such information by exploiting vulnerabilities in the organizations' personnel and information systems, will be capable of quickly and broadly disseminating classified government information before being detected. In a 2018 OIG report, we identified instances in which FBI employees, unable to pass multiple polygraph examinations, were allowed to retain access to sensitive information, systems, and spaces for extended periods of time without required risk assessments — potentially posing a security risk to the FBI. Further, a 2017 OIG report found that the FBI could improve its program for deterring, detecting and mitigating malicious insider threats, by ensuring that leads and referrals concerning insider threats are handled in a more systematic way.

To assist the Department in addressing its challenges related to national security, the OIG is conducting audits of the FBI's oversight of national security-related undercover operations; the BOP's counterterrorism efforts; and the FBI's efforts to identify homegrown violent extremists.

PROTECTING THE NATION AND THE DEPARTMENT AGAINST CYBER-RELATED THREATS

Cyber-related threats have the potential to adversely impact elections, the economy, and national security. As both a law enforcement agency and an agency that contains Intelligence Community elements, the Department has an integral role in protecting the nation against these threats. The Department serves as both the lead federal agency in investigating and prosecuting cybercrime and as one of the agencies responsible for warning state and local officials about cyber threats to the nation's election infrastructure. In addition, as a repository of national security information, law enforcement sensitive information, and other sensitive information, the Department must ensure that its own information systems are secure.

Investigating and Prosecuting Cybercrime and Other Crimes Facilitated Through Encryption Technologies

The Department faces challenges in investigating and prosecuting cybercrime, including activity on the "dark web," and in accessing or obtaining intelligible information in a form it can use due to the use of end-to-end encryption, also known as "lawful access."

The Dark Web. The investigation and prosecution of illegal activity on the "dark web" continue to be significant challenges for the Department. The dark web, or DarkNet, refers to a part of the Internet that is purposefully hidden, meaning that it has been designed specifically for anonymity. Users access the DarkNet with software that allows them to hide their true location and identity. Substantial illegal activity occurs on the dark web as offenders use the anonymity of this global platform to engage in serious transnational crimes, including the sexual exploitation of children, arms trafficking, identity theft, and narcotics trafficking. Despite these ongoing challenges, the Department has had some recent success investigating DarkNet crime that highlighted the importance of working cooperatively with other federal agencies and foreign law enforcement counterparts. To assist the Department in addressing this challenge, the OIG is currently examining the FBI's implementation of its dark web strategy and efforts to disrupt illegal activities.

Lawful Access.[4] The Department also faces challenges in investigating and prosecuting criminal activity facilitated through encrypted communications, including cybercrime. Many communications services and technologies are deploying end-to-end encryption with no lawful access solution. As a result, law enforcement agencies may not be able to access information about ongoing criminal activity or national security threats, even with a court order, because the information can only be decrypted by the end user. When reviewing its strategic objectives, the Department found that if it is unable to lawfully obtain evidence of criminal offenses and information concerning potential terrorist attacks due to end-to-end encryption, its ability to conduct criminal and national security investigations is hampered and the risk to public safety is increased. To address this challenge, the Department is considering a number of potential options, including the continued engagement with technical experts to seek access to encryption messaging platforms as well as the continued development and improvement of procedures for the increased use and deployment of sensitive investigative technologies. As the use of increasingly sensitive and intrusive techniques is required to overcome the lawful access challenge, the Department will need to take steps to ensure that its activities comply with all applicable laws, policies, and procedures.

Source: FBI

Election Security

The investigation and prosecution of cybercriminals are significant parts of the Department's effort to combat election interference. The Department is also responsible for working with state and local governments to ensure that the nation's election infrastructure is safe from cyberattack. The Department faces challenges in effectively coordinating with state and local governments to enhance election security, including challenges in providing sufficient cyber threat-related information to state and local governments. As noted in Volume I of the bipartisan Senate Select Committee on Intelligence (SSCI) Report on Russian Active Measures Campaign and Interference in the 2016 U.S. Election, the U.S. intelligence apparatus is designed to be foreign-facing, with limited domestic cybersecurity authorities except in specific instances, such as the FBI's ability to work with state election officials, who have primacy in running elections. The report found that, from 2014 and through 2017, Russian efforts exploited the seams between federal authorities and capabilities, and protections for the states to direct extensive activity against U.S. election infrastructure at the state and local level. Although the FBI provided actionable cyber threat warnings to the states in the late summer and fall

[4] In previous Top Management and Performance Challenges reports, this challenge was referred to as "going dark."

of 2016, the SSCI report found that the warnings did not provide sufficient differentiation between warnings specific to election infrastructure and other warnings issued by the FBI.

Ensuring the Security of Department Information Technology Systems

In addition to preventing and detecting insider threats as it relates to *National Security*, the Department also faces challenges protecting its information systems against internal and external threats more generally. To protect against these threats, federal law and policies require agencies to take a risk-based approach to cybersecurity by effectively identifying, prioritizing, and managing their cyber risks. Each year, the OIG assesses the effectiveness of the Department's information security program and practices, as required by the Federal Information Security Modernization Act (FISMA). Each evaluation must include: (1) testing the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems; (2) an assessment (based on the results of the testing) of compliance with FISMA; and (3) separate representations, as appropriate, regarding information security related to national security systems. For FY 2018, the OIG found deficiencies in the IT security of several critical Department components, including United States Attorney's Offices, the Criminal Division, and the FBI. The OIG made several recommendations to improve the information security programs within these and other components.

The OIG is continuing to conduct oversight work in the area of cybersecurity, including its annual FISMA audits and its assessment of the Department's implementation of the Cybersecurity Information Sharing Act of 2015 (CISA), which is being conducted jointly with the Inspectors General of the Departments of Commerce, Defense, Energy, Homeland Security, Justice, Treasury, and the Intelligence Community.

MANAGEMENT OF SENSITIVE INVESTIGATIVE AUTHORITIES

The Department is empowered to use certain sensitive investigative tools, such as confidential sources, bulk data collection, and conducting surveillance pursuant to a court order under the Foreign Intelligence Surveillance Act (FISA). These tools pose risks if they are employed without adequate management and oversight. Recent and past OIG reviews have found that the Department faces challenges in using these sensitive authorities consistent with its policies, and in a manner that safeguards individuals' statutory and constitutional privacy rights. The actual or perceived misuse of such authorities can undermine the public's trust and confidence in the Department, impact the Department's standing with the judiciary, threaten the success of prosecutions, and lead to the amendment or revocation of certain authorities.

Confidential Sources

Confidential sources serve as important investigative resources, but their management and oversight is a challenge for the Department because the sources most often have mixed motives, including their own self-interest, for cooperating with law enforcement; this can affect their reliability. The OIG has found over the course of several audits that the Department's management and oversight of confidential source programs has been inadequate. In audits issued in 2015 and 2016, the OIG found that the Drug Enforcement Administration's (DEA) confidential source program had insufficient management, controls, and oversight, lacked adequate governing policies, and did not adequately provide for the ability to evaluate source reliability. Additionally, in 2017, we found that DEA agents did not fully account for the risks associated with using and paying certain confidential sources and maintained poor documentation of source authorization, activity, and payments. For example, DEA policy prohibits paying sources who were deactivated because of an arrest warrant or for committing a serious offense, yet the OIG found that the DEA had paid about $9.4 million to more than 800 previously-deactivated sources between FYs 2011 and 2015. In the OIG's 2017 audit of the Bureau of Alcohol, Tobacco, Firearms and Explosives' (ATF) use of confidential sources, we also identified serious concerns, such as an insufficient review and approval process for higher-risk confidential sources who require additional oversight, and the agency's inability to efficiently identify and track total payments made to individual confidential sources. The OIG found there was a significant need for greater oversight and improved documentation to prevent such problems. Since the issuance of the above reports, the DEA and ATF have taken actions to address most of the OIG's findings and recommendations. The Department must remain vigilant in its use and management of human sources to appropriately account for the risks associated with this sensitive law

enforcement tool. The OIG is currently conducting an audit of the FBI's confidential human source program, with the report expected to be released during November 2019.

Bulk Data Collection and Other Privacy-Related Issues

The Department also faces challenges balancing the need to collect and exploit large amounts of data with the need to protect individual privacy rights. For example, in the OIG's 2019 review of the DEA's use of administrative subpoenas to collect or exploit bulk data from telecommunications service providers and other vendors, we found it troubling that the DEA proceeded with three such programs without sufficient legal analysis of its limited, drug-related administrative subpoena authority, which was applied expansively in two programs, and failed to have adequate procedural safeguards for these two programs. The DEA collected tens of thousands of records in one program without developing a plan for the disposition or retention of the data, which created a risk that information about individuals unconnected to illegal activity would be retained by the DEA for an indefinite time period.

In another example, the Government Accountability Office (GAO) examined the FBI's use of automated face recognition technology and made several recommendations to help ensure accuracy, improve transparency with the public, and safeguard the privacy of individuals whose photos are in the FBI's and external partners' systems. The FBI has taken actions to address and close four of the GAO's six recommendations regarding the FBI's use of face recognition technology and is taking steps to address the remaining two recommendations. However, as the exploitation of bulk data becomes increasingly necessary to the FBI's operational activities, it is imperative that the FBI continues its efforts to protect the privacy rights of the individuals whose data is collected.

The Foreign Intelligence Surveillance Act


Source: ATF

The Department faces challenges appropriately implementing its authorities under section 702 of the Foreign Intelligence Surveillance Act (FISA). In a declassified Foreign Intelligence Surveillance Court (FISC) opinion from October 2018, which was upheld in part by a July 2019 opinion from the Foreign Intelligence Surveillance Court of Review, the FISC noted that, since April 2017, the government has reported a large number of FBI queries that were not reasonably likely to return foreign-intelligence information or evidence of a crime, despite FBI procedures requiring that each query of FBI systems containing certain FISA information must be "reasonably likely to retrieve foreign intelligence information" or evidence of a crime unless otherwise specifically excepted. Further, the Court noted that in a number of cases, a single improper decision or assessment resulted in the use of query terms corresponding to a large number of individuals, including U.S. persons. In addition to these issues described by the FISC with

implementation of FISA section 702 authorities, the OIG is separately examining the Department's and the FBI's compliance with legal requirements, and with applicable DOJ and FBI policies and procedures, in applications filed with the FISC to conduct FISA surveillance of a certain U.S. person.

Proactive risk management and consistent oversight concerning all sensitive authorities are essential to the continued use of these important investigative tools. For example, the Department has responded thoughtfully and appropriately to past OIG reviews finding issues with the management of sensitive investigative authorities. In 2007 through 2016, the OIG issued eight reports regarding the FBI's use of National Security Letters and USA PATRIOT Act section 215 authorities. Corrective action taken by the FBI as a result of the OIG's recommendations substantially enhanced oversight of the use of these investigative tools and reduced the risk of their misuse. In order to effectively address this challenge, the Department must enhance the oversight of its use of sensitive authorities and proactively address issues that it identifies.

To assist the Department with its efforts, the OIG will continue its oversight of these authorities. The OIG's ongoing work in this area includes audits of the DEA's income generating undercover operations program, the FBI's covert contracting activities, and the FBI's national security undercover operations, and as noted above, the FBI's confidential human source program.

LAW ENFORCEMENT COORDINATION AND COMMUNITY ENGAGEMENT

The Department's top law enforcement priorities, which include combatting the opioid crisis, reducing violent crime, and investigating cross-border criminal activity, are most effectively addressed through cooperation among federal agencies, partnerships with state, local, and tribal law enforcement agencies, and engagement with impacted communities. Below, we detail some of the challenges the Department faces in addressing these law enforcement priorities.

Combatting the Opioid Crisis

The current opioid crisis is one of the worst drug epidemics in U.S. history. According to the Centers for Disease Control and Prevention (CDC), in 2017 the United States experienced 70,237 overdose deaths, of which 47,600 (67.8 percent) involved an opioid, averaging 130 opioid overdose deaths each day. Although the Department has created several programs and initiatives specifically designed to combat the opioid crisis, it still faces challenges in stopping the diversion of pharmaceutical opioids to unauthorized users and in assisting communities negatively impacted by the crisis.[5]

Preventing Diversion. In its September 2019 report examining the DEA's regulatory and enforcement efforts to control the diversion of opioids, the OIG found the DEA was slow to respond to the significant rise in the use and diversion of opioids since the early 2000s. Specifically, the DEA authorized a 400 percent increase in oxycodone production between 2002 and 2013, and it was not until 2017 that the DEA significantly reduced the oxycodone production quota, by 25 percent. To assist the DEA in preventing a similar health care crisis from occurring in the future, the OIG recommended that the DEA revive a drug abuse warning network to identify emerging drug abuse trends and new drug analogues and respond to these threats in a timely manner.

We also found that DEA policies and regulations did not adequately hold registrants accountable or prevent the diversion of pharmaceutical opioids. Our report recommended that the DEA require criminal background investigations of all new registrant applicants; that the DEA take steps to ensure that DEA diversion control personnel responsible for adjudicating registrant reapplications are fully informed of applicants' history; and that field division work plan requirements allow the flexibility to target registrants for investigation.

[5] The DEA is responsible for ensuring that all controlled substance transactions take place within the closed system of distribution established by Congress under Titles II and III of the Controlled Substances Act of 1970. When controlled substance transactions fall outside the closed system of distribution, the activity constitutes diversion.

Further, we found that the DEA does not adequately collect, maintain, or analyze data in order to identify trends in the use of controlled substances. Specifically, the DEA does not track ordering patterns for all pharmaceuticals, which could enable the diversion of these prescription drugs and compromise public safety. The OIG recommended that the DEA implement electronic prescribing for all controlled substance prescriptions, and that it develop a national prescription opioid enforcement strategy that encompasses the work of all DEA field divisions tasked with combating the diversion of controlled substances, and establish performance metrics to measure the strategy's progress. In addition, we found that the DEA's electronic system to collect suspicious orders was incomplete – it contained reports from only eight of the approximately 1,400 registered manufacturers and distributors that are required by federal law to send such reports to the DEA. The OIG recommended that DEA require that all suspicious order reports be sent to DEA headquarters.

Assisting Affected Communities. In FY 2019, the Department awarded $320 million in grants to combat the opioid crisis. Much of this grant funding was awarded through grant programs that provide financial and technical assistance to state, local, and tribal governments to identify, treat, and support individuals impacted by the opioid crisis, such as the Opioid-Affected Youth Initiative and the Comprehensive Opioid Abuse Site-based Program. However, as discussed below in the *Grants* section, the Department faces challenges in administering and overseeing grants, including in documenting progress towards the achievement of grant goals. The OIG is conducting an audit of the DEA's community-based efforts to combat the opioid crisis. Among other things, we are examining the DEA's efforts to sustain progress in the communities it assists, the DEA's integration of a performance measurement strategy to enhance its community-based efforts, and its collaboration with other agencies in combatting the opioid crisis.

While the Department and the DEA are taking steps to address the opioid epidemic, including increasing enforcement staffing and enforcement actions, and working more closely with communities and federal and state partners, challenges still remain.[6]

[6] For example, the Department assigned more than 300 federal prosecutors to U.S. Attorneys' offices (many of which are assigned to work opioid cases), hired more than 400 DEA task force officers, announced the formation of Operation Synthetic Opioid Surge to reduce the supply of deadly synthetic opioids in counties with high rates of synthetic opioid overdose deaths, announced the creation of the Appalachian Regional Prescription Opioid Strike Force to target doctors and pharmacies illegally distributing prescription opioids in nine districts, created a new initiative called the Opioid Fraud and Abuse Detection Unit to provide data analytics to all U.S. Attorneys' Offices for targeting the illegal distribution of opioids by healthcare professionals, and funded Opioid Fraud and Abuse Detection prosecutors in 11 "hot spot districts."

Reducing Violent Crime

In 2017, the OIG issued a review of the Tribal Law Enforcement Efforts pursuant to the Tribal Law and Order Act of 2010 (TLOA) that requires the Department to provide legal and investigative assistance to tribes. The OIG found that the Department has taken some steps to carry out TLOA's mandates, but challenges still remain.

Ensuring the safety of our communities by reducing violent crime continues to be a critical challenge area for the Department. In order to address this challenge area, the Department must maintain effective partnerships with other federal, state, local, and tribal law enforcement agencies, and ensure that it shares information effectively with these stakeholders. To assist the Department, the OIG is reviewing the Department's strategic planning and accountability measures for 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 experiencing significant increases in homicides and gun violence.

Preventing the illegal trafficking of firearms is an element of the Department's strategy to reduce violent crime. To that end, ATF develops and disseminates actionable crime gun intelligence through the Crime Gun Intelligence Centers (CGIC) across the country. The CGIC uses crime gun data from ATF's National Integrated Ballistics Information Network (NIBIN), firearms tracing, and industry inspections to generate actionable intelligence leads for federal, state, and local law enforcement. A 2019 OIG review found that ATF's Frontline business model initiative, enacted in 2013, expanded intelligence-gathering abilities of CGICs; however, policies and guidance have not kept up with the CGIC's evolving role, and outdated guidance may limit the development of individual CGICs. The OIG also found that ATF could improve promotion of the use of NIBIN and firearms tracing to its external partners to increase actionable intelligence. The OIG made several recommendations to improve the effectiveness of the Frontline business model initiative overall, including the positive impact that CGICs and the NIBIN can make on public safety.

Investigating Cross-Border Criminal Activity

Effective cooperation between the Department and Department of Homeland Security (DHS) components, such as Immigration and Customs Enforcement (ICE), is critical to the Department's ability to investigate crimes along the Southwest border. Despite this fact, coordination with ICE on investigations of cross-border criminal activity has been an ongoing challenge for the Department. In its September 2012 review of ATF's Operation Fast and Furious, the OIG found that ATF resisted efforts by ICE to conduct independent or coordinated investigations involving gun trafficking to Mexico. More recently, in a July 2019 joint review with the DHS OIG regarding cooperation between the FBI and ICE's Homeland Security Investigations (HSI) involving criminal activity at the nation's Southwest border, we found that over one-third of special agents who responded to our survey reported cooperation failures between the FBI and HSI. Specifically, we found that lack of cooperation between the FBI and HSI resulted in negative impacts, including lost trust in the other agency or its personnel, unnecessary use of resources, failure to gather evidence, or failure to apprehend a target. To assist the Department in accomplishing its strategic objectives in this critical law enforcement priority area, the OIG made a number of recommendations designed to improve cooperation between FBI and HSI along the Southwest border. These recommendations included developing written, agency-specific deconfliction guidelines; increasing awareness among FBI and HSI agents of each agency's mission, statutory authorities, and criminal investigative priorities; instituting an interagency Memorandum of Understanding for investigative interactions; and resolving unclear jurisdictional areas.

The OIG has two ongoing reviews related to the Department's immigration enforcement efforts: (1) a review of the Department's planning and implementation of its Zero Tolerance Policy relating to prosecution of persons for entering the U.S. illegally in Southwest border jurisdictions; and (2) a review of actions taken by the Department, including the Executive Office of Immigration Review and the BOP, to expand the Institutional Hearing and Removal Program—a joint DOJ/DHS program that identifies potentially deportable foreign-born inmates in federal, state, and local prisons and begins removal proceedings against those inmates.

ADMINISTERING AND OVERSEEING CONTRACTS AND GRANTS

In FY 2018, the Department obligated over $8.1 billion in contracts and awarded approximately $5.5 billion in grants. Although the Department has made some recent improvements to its administration and oversight of contracts and grants, we identified continued deficiencies in these areas, which present significant fraud and mismanagement risks.

Contract Administration and Oversight

The Department faces challenges in effective contract administration and oversight. Through our audit work, the OIG has identified certain recurring issues, indicating that Department components need to be more attentive in the following areas.

Compliance with the Federal Acquisition Regulation (FAR). The purpose of the FAR is to ensure that standard, consistent processes are used by executive agencies to procure goods and services in a fair and cost-effective manner. Over numerous contract audits, the OIG has identified FAR compliance problems, such as those described below, that have resulted in inefficient and unauthorized expenditure of taxpayer dollars. The OIG has consistently identified these issues in connection with specific contract audits, and recommended that the Department take steps to enhance awareness of FAR requirements and ensure that components are adhering to them. While the Department has taken actions to address many of the findings and recommendations in the specific OIG reports referenced below, the OIG continues to make similar findings and recommendations in its contract audits. As a result, the OIG remains concerned that there are systemic issues that the Department must evaluate and correct in order to improve its FAR compliance.

- Inadequate Documentation. The OIG has found multiple instances of lack of required documentation, ranging from inadequate contract files concerning the FBI's market research regarding fair and reasonable pricing in the 2017 OIG audit of an aviation contract to the absence of required documentation supporting the BOP's decision to award a dental services contract in another 2017 audit. In addition, the FAR requires agencies to document a justification for the use of contract types other than firm-fixed-price (FFP) because FFP contracts place responsibility for cost control and performance on the contractor. The FAR further urges agencies to continually re-evaluate whether non-FFP contracts can be transitioned to FFP or other lower risk contracts over time as experience provides a basis for firmer pricing. Yet, the OIG found that the DEA did not comply with these requirements in a 2018 audit of an aviation support contract. The OIG found similar non-compliance by the United States Marshals Service (USMS) in a 2018 audit of a court security officer procurement contract.

- Sole-Source Justifications. Because the FAR generally promotes full and open competition, written, certified, and agency-approved justification is required before negotiations can begin on a sole-source contract.[7] We have found that Department components do not consistently follow these regulations. For example, in a 2017 audit of a USMS sole-source contract awarded for detention services, we found that the sole source justification did not include all of the written support required by the FAR, which made it difficult to determine whether the decision to limit competition was appropriate. In addition, in a 2019 audit of a BOP sole-source contract for perimeter security upgrades at a U.S. Penitentiary, BOP officials acknowledged that other companies existed that may have been able to install the same fence, potentially at a lower cost. Given the substantial monetary value of the Department's contracts, it is essential that they are subject to competition to ensure value for taxpayers, or if a sole-source contract is warranted, that justification for it is documented and approved in accordance with FAR requirements.

Source: DOJ

- Prohibition on Personal Services Contracts. Several of our recent audits have revealed that current practices in the Department are potentially placing some contractor employees in a personal service role, exceeding the Department's statutory authority for those contracts. For example, an April 2018 OIG audit recommended training at the DEA to address this problem, and an October 2018 OIG audit recommended more robust procedures and policies at the Justice Management Division (JMD) to address it; the recommendations concerning personal services contracts have Department-wide applicability.

- Labor Law Compliance Concerns. The FAR requires that other applicable laws and statutes, such as labor laws, be followed. Nevertheless, the OIG has completed several audits where wage and fringe benefit rates for contract workers were not properly included in the contracts, as required under the Service Contract Labor Standards (SCLS), a federal labor regulation. We have also found contractors not meeting their obligations to employees or improperly classifying their employees as independent contractors and thus avoiding their obligations under federal labor laws or regulations. In addition, our audits have revealed multiple instances where contractors received price adjustments that were not warranted or exceeded the allowable increases for wages or fringe benefits. For example, in a 2017 audit, the OIG found that the USMS

[7] A sole-source contract is a contract for supplies or services that is proposed or entered into by an agency after soliciting and negotiating with only one source.

inappropriately approved a contract price adjustment that the contractor was not eligible to request and, as a result, the USMS paid the contractor a significant amount in unallowable costs.

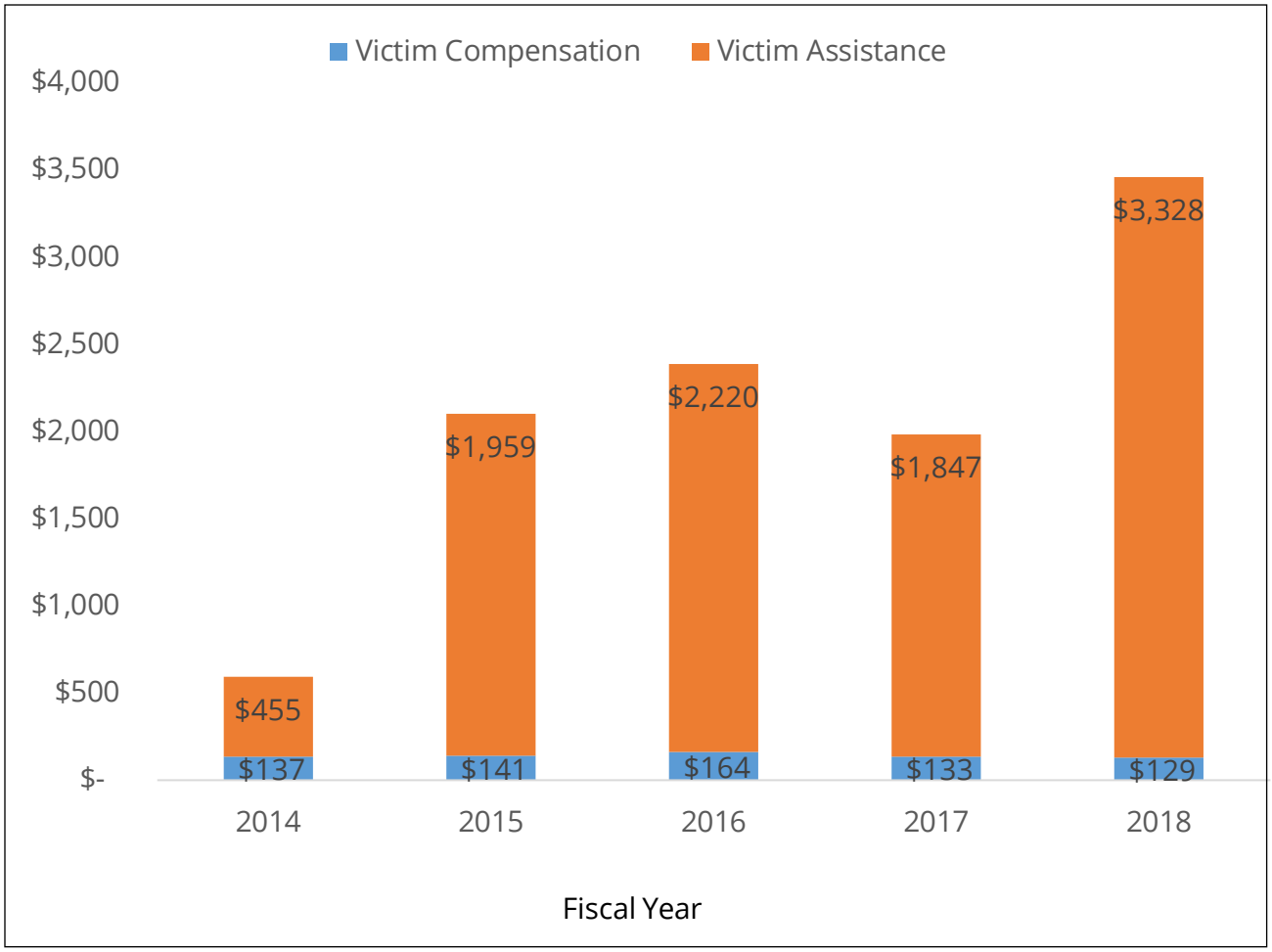
Contract Planning and Drafting. In our contract audit work, the OIG has found repeated instances of contract documents with unclear or poorly-defined requirements, which impeded the Department's contract administration. For example, a 2018 audit of a sole-source contract found that the BOP did not adequately plan for its construction project prior to awarding the contract. The BOP did not consult with subject matter experts on the needs of the prison, such as programming, food services, and health services, until after the contract was awarded, which led to a failure to include detailed construction requirements related to those needs in the contract's applicable conditions section, despite concerns from the Warden. The BOP's failure to anticipate significant problems with its plan caused it to pay over $1.7 million of taxpayer money to construct a building that was ultimately unnecessary. In addition, a 2018 audit of a DEA linguist services contract found the DEA had poorly defined contract requirements, which contributed to performance deficiencies.

Grant Administration and Oversight

Recent OIG grant audits have identified systemic grant administration and oversight challenges for the Department and its grantees, including in grant monitoring, controls over funds, documentation of progress towards achievement of grant goals, and compliance with award conditions. Specific areas of concern include the Department's challenges in managing awards made from the Crime Victims Fund (CVF); administering its non-CVF grant awards effectively; and monitoring grants to ensure safety of Department grant program participants.

Crime Victims Fund (CVF). In FY 2015, Congress more than tripled the amount of CVF funds available for distribution by the Department to support victims. As shown below, awards for CVF victim assistance and compensation programs rose from nearly $600 million to $2.1 billion in FY 2015. By FY 2018, awards for these programs totaled nearly $3.5 billion. The OIG has received $10 million from the CVF each year since 2015 to conduct oversight of the Department's awards for victims and victim services. As a result, the OIG has conducted numerous audits of CVF grant recipients. The Office of Justice Programs (OJP) awards the bulk of CVF grant funds to states and territories. We have observed several recurring issues that warrant the Department's attention to ensure proper administration and oversight of this substantial grant award program.

CVF Assistance and Compensation Grant Totals, in Millions
FYs 2014-2018



Source: OJP, OIG

For example, a 2019 OIG report on OJP's efforts to address challenges in administering CVF Programs found some states had difficulty adhering to spending requirements as a result of ambiguous and evolving CVF grant expenditure criteria, and also struggled to implement efficient subgrant strategies due to uncertainty regarding future annual CVF award amounts. The report also found some states struggled to monitor assistance subgrants, especially as the number of subrecipients and total CVF award amounts grew. Additionally, the report found as of March 2019, five OJP grant managers each managed an average of over $1.5 billion in CVF formula and discretionary grants, presenting a challenge to adequate monitoring. We recommended that OJP assist states in developing spending plans, assessing risk among subrecipients, and monitoring the service providers that ultimately receive the majority of CVF grant funds. We also prompted OJP to better define and communicate grant rules to the states, develop customized guidance for scenarios unique to the CVF programs, and improve its performance reporting process to reduce the risk of inaccurate data showing the effect of these programs.

Effective Grant Administration and Oversight. The Department also faces challenges in effective administration of its non-CVF grant awards and management of its grant processes. A 2018 audit of the Department's grant award closeout process—a process by which grant recipients submit documentation to the awarding agency to verify grant expenditures and performance—found that while the Department made progress in agency closeout timeliness, over $28 million in funding remained obligated against awards eligible for closeout. This included over $1.4 million in funding obligated to organizations that had not been operational for as many as 10 years. In these instances, the Department did not efficiently identify funding returned by its grantees or left unspent past the close of awards. We recommended that the Department's granting components develop policies and procedures to more promptly identify balances persisting on awards past their expiration and remedy these amounts by putting them to better use. A 2019 audit of the National Institute of Justice's (NIJ) overall management of its grants found the NIJ needed to improve how it administers awards and communicates with recipients. For example, the report found that NIJ social science analysts took actions that overlapped with NIJ grant managers' responsibilities, leading to improper communications from NIJ to grantees regarding consultant arrangements, supplemental funding, and the scope of certain awards. The OIG recommended that NIJ promulgate clarified position descriptions for its personnel and establish procedures to ensure appropriate communication with its grantees.

Grant Monitoring to Ensure Safety of Department Grant Program Participants. The Department's challenges in conducting effective grant oversight applies to areas beyond preventing mismanagement of taxpayer dollars. For example, a 2019 OIG audit of efforts to safeguard minors in the Department's youth-centered programs found the Department had a lack of specific guidance and formal award requirements for grantees regarding background screening of individuals participating in Department grant programs who are in direct contact with children. The absence of a consistent monitoring regime to determine what steps grantees took to screen individuals working with children put children participating in Department grant programs at risk. The OIG's 2019 audit of an OJP research grant awarded to Cincinnati City School District provided an example of a grant award in which this lack of guidance and monitoring resulted in a problem. That audit found the grantee had an insufficient background check process, which ultimately resulted in individuals with criminal records—involving trafficking drugs near a school and endangering children—participating in a grant program that involved their escorting children to school. The OIG has recommended that the Department articulate screening requirements for grant programs that may involve contact with minors, leverage existing law enforcement tools to facilitate screening, share training and techniques for child abuse prevention, and enhance its monitoring of grantees' background screening processes.

The OIG is continuing its contract oversight work and grant audits to assist the Department in meeting these challenges.

USING PERFORMANCE-BASED MANAGEMENT

Performance-based management is an approach that establishes strategic program goals, with progress toward achieving those goals being determined by reference to relevant objective measures, and uses the collection, review, and analysis of data to evaluate performance and performance improvement.[8] This approach enables assessment of the impact of the Department's programs, proactive identification of areas of risk, and informed resource allocation and decision making. Many Department components lack either meaningful performance goals and measures or the data necessary to evaluate their programs. Although the Department is working to improve its performance management processes, including improving the accuracy and reliability of its data, significant challenges remain.

Performance Goals and Measures

As the OIG conducts audits and reviews of Department programs, it evaluates the extent to which decisions about whether a program is successful are determined by performance-based measures. Over the past year, the OIG has identified inadequate performance goals in several programs across different components of the Department, including ATF's Frontline Initiative, the BOP's contracted substance abuse treatment and mental health services, the DEA's efforts to control the diversion of opioids, and the Office on Violence Against Women's (OVW) Training and Technical Assistance Program. In order to address this issue, the OIG recommended that the Department develop performance metrics to assess the overall effectiveness of these programs.

Data Collection and Reliability

The Department faces challenges in collecting the data necessary to measure program performance, including the fact that some of the data the Department needs is unavailable. As noted in a text box in the *Prisons* section, a 2017 Procedural Reform Recommendation determined that the BOP had incomplete healthcare claims data in electronic format and that the claims adjudication vendor had not provided all contractually required services, including fraud monitoring. The OIG found that, as of February 2017, only 16 of the 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 the BOP's

[8] The Government Performance and Results Act Modernization Act of 2010 and corresponding guidance from the Office of Management and Budget's Circular A-11 establish the framework for performance-based management. The Act requires federal agencies to establish and publish general goals, as well as priority goals, and complete periodic assessments of progress toward each goal. The Foundations for Evidence-Based Policymaking Act of 2018, signed into law in 2019, expands upon this effort by directing federal agencies to assess the effectiveness and efficiency of their programs using systematic data collection and analysis.

health care contracts manually in a paper-driven process and, as a result, billing activity could not be analyzed in any meaningful way. Further, a 2018 OIG report found that despite the *Death in Custody Reporting Act of 2013* (DCRA) requirement to begin collecting data about law enforcement-related deaths and deaths in correctional institutions, not all federal law enforcement agencies are submitting the data, and the Department is not collecting state data. Without complete information about deaths in custody, the Department will be unable to achieve DCRA's primary purpose—to examine how DCRA data can be used to help reduce the number of deaths in custody. Multiple other OIG reviews have also found the Department's data to be incomplete and inaccurate, including data related to foreign nationals sponsored by the Department, the FBI's cyber victim notification process, and grant recipient activity funded by the Crime Victims Fund.

Moreover, even when relevant data may be available, the OIG has found, in some of the above-noted reports and otherwise, that the Department's components have not adopted a performance-based management approach in that they have not identified program goals by reference to relevant objective measures.

To assist the Department in addressing its ongoing challenges related to performance-based management, the OIG will continue to assess the Department's ability to collect and use data to measure program effectiveness, inform decision-making, and improve outcomes as part of its oversight of Department programs and operations.

FOSTERING A DIVERSE, HIGHLY-SKILLED WORKFORCE

The Department faces a number of challenges in its efforts to ensure that it has a diverse, highly-skilled workforce with the expertise necessary to accomplish its mission. These include challenges related to recruiting and retaining employees to fill certain mission critical positions, and to ensuring that the Department's specialized expertise and institutional knowledge is not lost through retirement.

Recruitment and Retention

The Department faces challenges in both recruiting and retaining employees in a highly competitive marketplace. The Department's efforts to recruit and retain skilled employees may be hindered by declining employee engagement, work-life balance concerns, and its lack of diversity in certain key positions.

Highly-Skilled Professionals. The Department faces challenges in recruiting and retaining employees to fill certain mission critical positions, such as healthcare and cyber-related positions. As noted in previous years' reports, healthcare professionals and cyber-professionals are highly sought after in the private sector and often receive salaries that cannot be matched with the federal pay scale. As a result, the Department must work within existing laws and regulations to provide compensation packages and work-life opportunities to remain competitive with the private sector.

The OIG has long expressed concerns about the BOP's inability to fill its healthcare positions. For example, in a 2016 report, the OIG found that only 83 percent of the positions in the BOP health services units were filled as of September 2014. The report noted that, as a result, inmates were sent to non-BOP medical providers to receive medical care, further contributing to increased inmate medical costs. The OIG further 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. In response to the review, the BOP enhanced its use of data to assess and prioritize medical vacancies and developed strategies to improve recruitment efforts. The remote locations of many of the BOP's facilities pose another challenge to the recruitment of medical personnel to the BOP. In the OIG's 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. Although the BOP is attempting to use available incentives to fill its vacant healthcare positions, this challenge persists.

In the cyber arena, the Department has acknowledged its difficulties in recruiting and retaining experienced cyber-professionals. For example, in its July 2018 report, the Attorney General's Cyber-Digital Task Force noted that the Department is constantly working to retain attorneys and investigators with cyber-related expertise and that it must find alternative incentives to recruit and retain those employees. As noted below, the Department must address its deficiencies in the non-monetary factors that affect recruitment, retention, and engagement of employees to remain competitive, particularly in the markets for health services employees and those with cyber expertise.

The Department also faces challenges in identifying vacant cyber–related positions. In a March 2019 report, the GAO found that the Department was unable to comply with the requirements of the Federal Cybersecurity Workforce Assessment Act of 2015 to identify filled and vacant positions within IT, cybersecurity, and cyber-related functions. The GAO found that by not completing its efforts to identify its vacant IT, cybersecurity, and cyber-related positions, the Department lacks important information about the state of its workforce. As a result, the Department's ability to identify work roles of critical need and improve workforce planning may be limited.

Employee Engagement and Work-Life Balance.

The Department faces challenges in the areas of employee engagement and work-life balance that may hinder the Department's efforts to recruit and retain highly-skilled staff. In its 2018 Federal Work-Life Survey Government-wide report, the Office of Personnel Management (OPM) found that work-life programs have a positive impact on recruitment, retention, performance, and employee morale. However, in the most recent OPM Federal Employee Viewpoint Survey (FEVS) results and Partnership for Public Service's (PPS) 2018 Best Places to Work in the Federal Government ranking, the Department scored below more than half of large federal agencies in the area of work-life balance. While work-life balance may be challenging given the nature of the Department's trial and investigative work, the Department should examine the extent to which it can make work-life programs and schedule flexibilities available to employees when the demands of their positions permit. In addition, in the past three years, the Department's employee engagement scores have declined in the rankings.[9] According to

In April 2019, the Attorney General signed an EEO statement that proclaims that the DOJ is an Equal Opportunity Employer that does not discriminate based on sexual orientation, gender identity, sex, pregnancy, parental and marital status, race, color, national origin, disability, and several other categories. Although all agencies are required by law to issue an EEO statement at the beginning of a new administration and every year thereafter, the DOJ had not issued a statement since March 2016.

[9] OPM defines "employee engagement" as "an employee's sense of purpose that is evident in their display of dedication, persistence and effort in their work or overall attachment to their organization and its mission."

the OPM, employee engagement scores are linked to employee retention and lower scores indicate employees are more likely to leave their places of employment.

Diversity. OPM has found that a diverse workforce has several benefits, including better informed agency decisions through consideration of varied perspectives, increased creativity and innovation, and an increased capacity to serve and protect people who have different experiences. To meet the goal of widening the talent pool available to the federal government, Executive Order (E.O.) 13583, *"Establishing a Coordinated Government-Wide Initiative to Promote Diversity and Inclusion in the Federal Workforce,"* directs the federal government to enhance its ability to recruit, hire, promote, and retain a more diverse workforce. The Executive Order further directs the federal government to create a culture that encourages collaboration, flexibility, and fairness to enable individuals to participate to their full potential. According to the 2018 Best Places to Work in the Federal Government rankings, the Department ranked 14 of 16 large agencies in support for diversity and ranked in the lowest quartile in this category for the second year in a row. In addition, according to the Department's FY 2018 Employment Fact Book, as of September 30, 2018, only 25 percent of the Department's Senior Executive Service was female.

Of particular concern is the lack of diversity in the Department's law enforcement components. According to OPM, law enforcement is an area where there is a critical need for civil servants who look like the people and communities they serve. However, in its 2018 report, a "Review of Gender Equity in the Department's Law Enforcement Components," the OIG found that women accounted for only 16 percent of Criminal Investigators in DOJ's law enforcement components. The OIG also found that women held few headquarters executive leadership positions over operational units and few top field leadership positions. While we determined that ATF, the DEA, the FBI, and the 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.

Succession Planning

The Department risks losing critical institutional knowledge if it does not have an effective human capital program that includes a talent management and succession planning process. As of September 30, 2018, approximately 28 percent of the Department's workforce was over 50. Given the Department has one of the youngest average retirement ages in the federal government (56.2 years in 2017), due in part to the mandatory retirement requirement of its law enforcement officers, it is likely that a quarter of the Department could retire within the next 10 years.

The Department's challenges in hiring and retaining a workforce with the specialized skills to accomplish its mission impacts the majority of the other top management and performance challenges that the Department faces. Therefore, it is imperative that the Department continue to improve its ability to recruit, attract, and retain top talent while planning for the seamless transition between its current leadership and the leadership it

will need to accomplish its mission in the future. In order to meet these challenges, the Department will need to pay greater attention to non-monetary factors, such as the diversity of its workforce, inclusion policies, employee engagement, and work-life issues.